International Comparative Legal Guides

Digital Health 2020

A practical cross-border insight into digital health law

First Edition

Featuring contributions from:

Advokatfirma DLA Piper KB
Astolfi e Associati, Studio Legale
Baker McKenzie
Biopharmalex
Bird & Bird LLP
Cliffe Dekker Hofmeyr
D'Light Law Group
GVA Law Office
Hammad & Al-Mehdar Law Firm
Herbst Kinsky Rechtsanwälte GmbH
Hoet Pelaez Castillo & Duque
Kemp Little LLP
Kyriakides Georgopoulos Law Firm
LEĜA
LexOrbis
Llinks Law Offices
Machado Meyer Advogados
Mason Hayes & Curran
McDermott Will & Emery LLP
OLIVARES
Polsinelli PC
Quinz
Gilat, Bareket & Co., Reinhold Cohn Group
Shook, Hardy & Bacon L.L.P.
The Center for Healthcare Economics and Policy, FTI Consulting
TripleOKLaw LLP Advocates
VISCHER

ICLG.com

ISBN 978-1-83918-027-9
ISSN 2633-7533

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Group Publisher
Rory Smith

Associate Publisher
James Strode

Senior Editors
Suzie Levy
Rachel Williams

Sub Editor
Lucie Jackson

Creative Director
Fraser Allan

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Digital Health 2020

First Edition

Contributing Editor:
William A. Tanenbaum
Polsinelli PC

©2020 Global Legal Group Limited.
All rights reserved. Unauthorised reproduction by any means, digital or analogue, in whole or in part, is strictly forbidden.

Disclaimer
This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.
This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Expert Chapters

Q&A Chapters

Digital Health, New Technologies and Emerging Legal Issues

Polsinelli PC

William A. Tanenbaum

Technology has always been how we practise medicine. The rapid development of new technologies has made Digital Health an important field in the advance of healthcare, and reflects the convergence of increased computing power, lower data storage costs, enhanced connectivity, and sophisticated data analytics.

These new technologies, such as 5G wireless networks and Data Fabrics, will give new reach and power to Digital Health; foster new regulations, such as for Software-as-a-Medical Device; enable new forms of patient care, such as telesurgery; and require new supporting IT infrastructure, such as Edge computing networks and the Internet of Medical Things ("IoMT"). These, in turn, necessitate upgrading healthcare technology and data agreements in the context of the multi-user, multi-vendor, multi-stakeholder environments that characterise the information technology ecosystem of hospitals and other healthcare institutions. (For convenience, healthcare institutions and healthcare providers will be referred to as "hospitals".) Joining law with Digital Health involves the transfer of innovative legal practices from healthcare to other industries and adopting the best practices of other industries into healthcare to take advantage of the opportunities and meet the challenges of using new technologies. Healthcare technology companies providing products and services to hospitals also need to be aware of these issues.

Digital Health *vs.* Digital Medicine

A framework for the relationship between Digital Health and Digital Medicine is provided by the Digital Therapeutics Alliance in a publication entitled "Digital Health, Digital Medicine and Digital Therapeutics (DTx): What's the Difference?".[1]

In this framework, Digital Health is defined as a category which includes technologies, platforms and systems that are used by health systems, clinicians, researchers, payers, patients and individuals for wellness and health-related purposes; for the collection, storage and transmission of health data; and in clinical procedures and the life sciences. Digital Medicine is considered a subcategory of Digital Health and includes hardware and software that measure or are used in providing healthcare interventions. Consumer-facing wellness, and fitness and lifestyle products and services, are generally considered to be in the Digital Health and not the Digital Medicine category. Digital Therapeutics (often referred to as "DTx") is a subcategory of Digital Medicine and uses evidence-based therapeutic interventions to prevent, manage or treat a medical condition.

As provided in the above framework, Digital Health encompasses the following categories:

1. Data and information collection, storage and presentation, including user-facing technologies such as lifestyle apps, fitness trackers, nutrition apps, medicine reminder apps and healthcare scheduling apps.
2. Health Information Technology ("HIT") such as electronic medical records systems and electronic prescribing and order entry systems.
3. Consumer health information such as online data repositories; personal health records; and provider-patient Internet portals.
4. Telehealth.
5. Decision support software, which provides information to clinicians for their independent review.
6. Enterprise support, such as clinical trial operations and management software and platforms.
7. Clinical care administration and management tools, such as those used for revenue cycle, clinical staffing and hospital length-of-stay management.

Digital Medicine includes the following categories:

1. Digital diagnostics, such as software-enabled connected devices that detect or confirm a medical condition.
2. Digital biomarkers, such as digital tools that measure medical characteristics and evaluate them as indicators of normal biologic or pathologic processes, or biological responses to a therapeutic intervention.
3. Digital clinical outcome assessments such as digital measurements of how patients feel and function.
4. Remote patient monitoring, medication adherence, and sensor technologies that measure vital signs and physiologic data.
5. Decision support software that processes and analyses data from medical images and often without initial input from clinicians.
6. Measurement and intervention products, such as a digital component integrated with a drug or biologic product, ingestible sensors, or connected drug delivery devices (such as insulin pumps).
7. Digital products that measure and intervene in medical care and do not require any human intervention, such as an artificial pancreas, a pacemaker, and a cochlear ear implant.

Digital Therapeutics deliver software-driven digital medical intervention to:

1. treat a disease;
2. manage a disease; and
3. improve a patient's health function and/or prevent disease.

General Overview of Digital Health Legal Issues

The legal issues that apply to Digital Health and Digital Medicine can be placed in a matrix which overlays the above framework.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

The legal issues from the hospital and healthcare provider perspective can be organised into the following categories:

1. Healthcare delivery and operations, including regulatory compliance, payment and reimbursement (including technologies for calculating and transmitting payments).
2. Regulatory compliance, including for the emerging regulatory frameworks for Software-as-a-Medical Device and other Digital Medicine technologies.
3. Technology agreements, including joint-development agreements between hospitals and healthcare technology companies, and agreements for moving from the pilot phase of a new technology to its validation and to its deployment throughout the hospital.
4. Cybersecurity for the Internet of Medical Things.
5. Data, including data protection, ownership, sharing, commercialisation, and establishing hospital data policies that meet, compliment or extend beyond regulatory requirements.
6. Data Analytics, AI, (including "AI-as-a-Service" ("AIaaS")), Machine Learning (a subset of AI), and natural language processing ("NLP").
7. Data privacy and cybersecurity, including GDPR (the General Data Protection Regulation) and in the U.S. HIPAA (the Health Insurance Portability Act, with its Security Rule and Privacy Rules for electronic health records) and the CCPA (the California Consumer Protection Act, which went into effect on 1 January 2020, and which has nation-wide applicability).
8. Intellectual Property, including allocating ownership and license rights between a hospital and multiple third party technology companies.
9. Electronic health records, including physician-patient electronic communications.
10. Financing, including for development, acquisition and operation of Digital Health technologies.
11. Liability for medical treatment involving AI.

Key Emerging Technologies in Digital Health

Three important technologies are 5G ("fifth generation") wireless technology for mobile networks, the Internet of Medical Things, and AI-enabled data analytics. These are discussed below, along with the legal issues they raise.

Is 5G Wireless Communications a Healthcare Revolution in the Making?

5G networks have the potential to provide faster, more robust networks and provide a wireless infrastructure for Digital Health. The migration from 4G ("fourth generation") to 5G networks can enable Digital Health technologies to advance patient care as well as reduce the costs of hospital operations. Compared with 4G, 5G brings three basic benefits to Digital Health. The first is increased speed to send and receive more data in the same time period. For example, 5G can be up to 100 times faster than 4G, which means 5G can increase speed from 1 GBps (gigabyte per second) to up to 100 GBps. The second advance is the reduction in latency from 10 milliseconds to 1 millisecond, which is a meaningful reduction. Latency is the delay in data transmission. In 4G networks, latency shows up as jitters or brief delays in videoconferences. Reduction in latency is a key differentiator between 5G and 4G. As a result, the connected devices in the Internet of Medical Things will be more responsive to each other and have to wait much less for receipt of the data necessary to perform their functions. With 5G networks, lower latency means medical images can be downloaded much faster to the point of care. The third advantage is greater bandwidth, which means many more devices can be connected at the same time. In healthcare, this increase in bandwidth means that more sophisticated devices, and more of them, will be able to connect to the network. It is important to emphasise that 5G is a wireless network technology, which means that healthcare can be provided over the Internet without the necessity of being hard-wired into a computer system.

Telehealth is a prime example of where 5G can meaningfully enhance Digital Health. 5G can overcome low bandwidth and slow speeds now experienced in providing telehealth. 5G can connect general practitioners with patients in rural areas or located far from hospitals or underserved areas. 5G also can increase the efficacy of video conferences for physician-patient visits especially when combined with the ability to upload and download diagnostics images in a few seconds during the teleconference. 5G can bring specialist medical care to victims in disaster zones and to patients in emergency situations where the requisite mobile networks are in place. Moreover, 5G-enabled medical care can address the physician shortage and hospital closures in low-population regions by alleviating the necessity of patients having to travel great distances to get their medical care. In short, 5G increases the capability of the virtual hospital model.

5G telehealth can also be used in hospitals within the same healthcare system to connect emergency rooms with specialists, and to connect doctors visiting a patient off the main campus with doctors and other healthcare providers at the main hospital. To oversimplify, 5G has the potential to make telehealth "boring" – that is, to so tightly integrate it with healthcare delivery as to make it unremarkable.

An extension of this remote telehealth is telesurgery. The technical capabilities of 5G networks, including high-definition image transmissions, will likely increase remote, robotic surgery done over the Internet. Most robotic surgery today involves the patient, the surgeon and the robotic equipment in fairly close proximity, although there has been telesurgery with the medical team in New York Hospitals and patients in European hospitals. 5G systems with high-speed, low-latency connectivity has the potential to provide surgery at a distance and allow highly skilled surgeons to provide treatment across the country and across continents. In addition, 5G wireless networks can be used to support advanced haptic technologies – technologies that provide a sense of touch – and touch to vision in performing operations. As with other forms of telehealth, 5G can help surgeons perform operations in disaster zones and during emergencies. Ambulances and other emergency vehicles when connected to 5G mobile networks will enable doctors to provide real-time guidance to first responders based on real-time medical information transmitted to the hospital from medical equipment operating in the vehicle.

Remote patient monitoring is another field where additional capabilities can be enabled by 5G. 5G will expand remote monitoring capabilities. It will enable the use of more sophisticated diagnostic and monitoring devices, including an array of wearable sensors. This has advantages where remote monitoring of chronic conditions is of value. 5G will enable more real-time, remote monitoring. Better patient monitoring allows faster interventions and, for this and other reasons, can also reduce hospital readmissions, and thereby provide cost advantages to healthcare systems. Related to patient monitoring is remote diagnostics and prescription monitoring. Next-generation patient monitoring technology will transmit data to the hospital for analysis by AI algorithms. It will also provide data sets for Machine Learning to further aid research and clinical treatment, such as, for example, training algorithms in identifying markers for medical conditions at an early stage.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Virtual Reality ("VR") and Augmented Reality ("AR") technologies will grow in utility as the speed and bandwidth of 5G adds more "reality" to these technologies. VR technology is used in rehabilitation and related recovery treatments. VR and AR are also used in training medical students and in preparation for surgical and other procedures.

Wireless Connectivity within the Hospital

5G wireless connectivity can be used within the hospital as well. It can be used as part of a mobile network to allow the use of complex diagnostic or treatment equipment when a wired network has limitations. In that sense, it provides on-demand access through a mobile system. 5G networks will allow MRI machines, X-ray machines and similar diagnostic machines to provide treatment benefits when they can be detached from wall hook-ups and made into mobile devices that be relocated as necessary for treatment within the hospital.

The Internet of Medical Things

Hospitals are increasingly installing connected devices that make up the institution's Medical Internet of Things. These devices include sensors that monitor the health of patients and assist in the design and delivery of health. One example is a smart hospital bed. It is a software-enabled, sensor-laden, connected device that collects, generates and exchanges data and can do so within regulatory requirements. It sends a patient's vital signs directly to the nurses' stations, and increasingly, to smart watches on the wrists of physicians. It collects and sends information to the hospital's Electronic Health Record systems. It sends other information to other hospital IT systems, and becomes part of a patient's IT "interface" with healthcare staff.

Other examples of IoMT are: smart bandages; implantables (such as pacemakers); ingestibles (such as digital diagnostic pills) and wearables (which provide a range of sensor technology); body area networks (which are a combination of the above); and virtual assistants such as Amazon's Alexa, which is HIPAA compliant under U.S. law with respect to data transmission.

Data Fabrics

Data analytics is an important part of Digital Health. Analytics relies on Machine Learning. In healthcare, "AI" means "augmented intelligence" rather than "artificial intelligence". Data analytics relies on Machine Learning, where algorithms improve by learning from datasets provided to them. One example is learning to identify malignant tumors in medical images. What is distinctive about healthcare is the role of people in training the algorithms: a limitation of Machine Learning is that it cannot weigh the impact of false positives or false negatives in the way that a doctor can, or make the judgment on when to err on the side of caution in making an analysis.

An obstacle to robust Machine Learning in healthcare is that data is generated by numerous databases, stored in different locations and in incompatible forms, and on multiple computers running different computer programs at different sites. A "Data Fabric" is a technology that supports improved analytics by addressing the problems of dispersed data and multiple computer programs. It accomplishes this by providing connectivity between the data in different locations, which is stored and processed by multiple computer programs. The relevant data is often stored in the Cloud as well as on hospital premises in its own servers.

The advanced functionality provided by Data Fabrics is the ability to connect not only data, but to connect both data and software, and at the same time leave the data and software in their original locations. This overcomes the need to convert the data to a common format in a combined database and eliminates the need to unify the computer programs required to use the data. Another way of framing this is to say that a Data Fabric is an IT architecture and a collection of IT data services (or functions) that coordinate the management of data stored in different sources.

An issue in Machine Learning is the difference between training data and current, real-world data. 5G networks will be able to "feed" real-world data to the algorithms, and thus can work with Data Fabrics to increase the efficacy of Machine Learning. As IoMT devices get smarter, Data Fabrics and other "smart" technology can assemble the data into comprehensive data sets that can be provided in the form of a unified stream of rich data that can enhance Machine Learning and the development of better algorithms.

Upgrading the IT Infrastructure and Emerging Legal Issues

New IT infrastructure is required to meet the demands and provide the benefits of data generated by 5G networks. One of these is Edge computing. In cloud computing, the computing is done in a terrestrial data centre connected to the customer over the Internet. The time it takes for the output from computer processing to get from the Cloud to the hospital device can be too long in time-critical situations. For example, in the case of wearable devices worn by patients, the lag – or latency – in transmitting the results of data processing can harm patient health. When machine-to-machine decisions have to be made in fractions of a second, the Cloud is too far away and too slow.

Edge computing addresses this. Edge computing refers to an IT infrastructure that puts computer processing as close to the data source as possible. In this case, a relevant source is the IoMT network, and the "edge" is physically close to the network so that the data can travel to and from the computers quickly. This allows faster processing and leverages Data Fabrics by allowing faster data analytics. From both an IT and legal perspective, edge computing is a new layer of IT infrastructure. Because it is a new technology, old forms of contracts may have weaknesses or omissions with respect to the requirements a hospital will want to impose on the edge computing vendors.

This architecture raises both security and privacy issues that lawyers and the IT department must address. The Internet of Medical Things must be the security of the Internet of Things. The devices themselves should have robust security, and the network part of connected devices must also have strong security. Otherwise, both the devices and the network can be pathways for cyberattacks. A related question is how the devices are updated with security patches. Must this be done one device at a time, or can all devices and networks be updated on a centralised basis by the IT department? The IT staff must conduct due diligence to ascertain this, and the legal department must draft the contract to require the vendor to validate security features upon initial installation and to provide, install and verify security updates throughout the contract term.

Emerging Legal Issues

1. Edge computing is a new form of IT infrastructure and old-form contract templates may be inadequate to address this technology in general and how it is deployed in the hospital environment in particular.
2. Gap Analysis: the fundamental question is whether existing IT contracts are out of date and whether they adequately

© Published and reproduced with kind permission by Global Legal Group Ltd, London

require existing IT vendors to provide the services the hospital needs to support its Digital Health technologies. These include IT infrastructure, data management agreements and master services agreements, and underlying SOWs and project plans. Baseline legal requirements should be established for the technology that is in place now or will be in place in the near future. Then a "gap analysis" should be performed to identify where contracts are not up-to-date, a risk assessment should be undertaken, and then the legal department should decide on whether to renegotiate the agreements, or replace them before expiration or the next renewal term begins. A common issue will be that the hospital's IT security requirement and privacy requirements will be increased but the agreements do not obligate the vendor to meet the current requirements.

3. Intellectual Property: in today's world, improvements are made on a collaborative basis by the vendor, the hospital, and often a third-party technology company. The statutory patent and copyright rules can give rise to unexpected adverse results in collaborative developments. The result is a need to address allocation of ownership and license rights in a comprehensive manner in the contracts.
4. Data use and data share agreements have increased in importance in the contract within the contours of the statutes and allocate ownership and license rights by contract. Current law has not developed blackline rules on intellectual property ownership of data and data analytics. These are therefore allocated by contract.
5. Liability for privacy violations under HIPAA, GDPR, and CCPA and other relevant statutory frameworks must be addressed. The "CCPA" is the California Consumer Protection Act, which came into force on 1 January 2020. It provides privacy rights and, while it is California state legislation, as a practical – and legal – matter, it generally applies on a nationwide basis.
6. The IT environment for mobile computing, 5G wireless networks, and new forms of vendor management must be adopted. Often the hospital needs acquire active cooperation among vendors.

Insights for Digital Health from Other Industries

Medicine's use of digital technologies overlaps with other industries' use of the same technologies. Other industries can provide best practices to be adopted and then adapted by the healthcare industry. For example, the quality of data analytics is dependent on the quality of the data, and for analytics purposes, "Big Data" is really "Big Metadata". Metadata is "data about data", and provides the attributes about the data file, and is one of the factors that enables data searches and data analytics. Moreover, data has a life cycle. Data elements change over time, and hospitals need systems in place to monitor the data cycle and determine when data may be out of date. The practices of industries with data-driven businesses can be instructive for healthcare. As one example, regulated industries such as the financial services industry have experience in building regulatory requirements into data policies when assembling databases. This also occurs, for example, in companies that use AI to perform predictive maintenance.

A hospital can have IT security without privacy, but it cannot have privacy without security. Hospitals' use of AI and Machine Learning makes data hygiene an important business practice. Hospitals should follow practices in other industries of using integrated risk management technologies and internal policies which have addressed the technology contracts with third-party service providers and business partners to protect data integrity. These consist of the following: identity assurance, to establish with a high degree of confidence that the person or entity or data element is what it purports to be; access assurance, which uses technology to determine who is authorised to access data; and activity assurance, which determines the scope of what an authorised person can and cannot do with that access. The financial services industry has developed robust technology and business practices that can serve as a model for hospitals. In addition, when a hospital uses a third-party service provider and a "RFP" (the Request for Proposal process), security starts with the RFP. RFPs generally use a scoring system based on points for different categories. If the hospital assigns lower points to data security, then the vendors competing for the business will give low priority to security when crafting their proposals.

Digital Health technology agreements often include a series of SLAs (the service levels to measure vendor performance) combined with a monetary credit in the nature of a penalty that is issued by the vendor to its customer when it (the vendor) fails to meet the performance requirements. In the case of persistent problems, a practice from outside of healthcare may be instructive. This is for the hospital and its vendor to declare "SLA holiday". During this period, credits are not issued while the vendor invests time and talent to conduct a root-cause analysis to get to the bottom of the problem instead of fixing it only in a manner sufficient to avoid having to issue credits.

The complexity of having multiple vendors and service providers creates challenges in vendor management. Other industries are experimenting with new forms of vendor management, one of which is similar to orchestrating vendors rather than using a managed service model.

Open source software is often favoured by academic medical institutions. However, deciding in theory to use "open source" means that, in practice, an institution has to decide which of the approximately nine open source models it wishes to use. A critical difference in the models is whether, under the specific form of open source model, patent rights can remain proprietary to the hospital or whether they will in effect be placed in the public domain in the sense that the open source license contains a free license to use patentable subject matter. The lessons from other industries is for healthcare institutions to develop two institutional open source policies. One is an internal policy that establishes rules as to which open source models are free to use, which are prohibited, and which require clearance. The second is an external policy that applies the same types of rules and procedures when the institution's departments hire, or go into partnership with, external software development companies. The goal of both policies is to prevent the institution from losing intellectual property rights under open source rules. Such a loss could undermine plans for the institution and its researchers to monetise intellectual property rights.

Healthcare can borrow intellectual property practices from industries where joint development agreements are commonly used for collaborative innovation. As noted, intellectual property statutes may allocate ownership and license rights in jointly developed intellectual property rights, in ways not consonant with the parties' business objectives regarding IP ownership and the allocation of licence rights. As a result, agreements must be tailored to cover the offensive and defensive aspects of intellectual property in the context of the short and long-term healthcare and business objectives.

Other areas where developed practices in other industries can be adopted or serve as models for Digital Health include: augmented reality and virtual reality; workflow automation; scaling large mobile networks; and technologies that have been used in industrial applications in other industries can be adopted.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Conclusion

The rapid development of Digital Health depends on a complex interplay of patient-facing technologies, clinical support technologies, regulations, data-driven decisions and the foundational IT infrastructure. 5G will bring a level of connectivity that will drive innovation. Data Fabrics address the problem of dispersed data and multiple computer programs. Edge computing reduces the latency of cloud computing and provides the speed required in a hospital setting. Digital Health's success will be a combination of innovation by healthcare institutions combined with the adoption of best practices used in other industries for the management of new technologies and in agreement structures.

Endnote

1. See https://dtxalliance.org/2019/11/11/digital-health-digital-medicine-digital-therapeutics-dtx-whats-the-difference.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

William A. Tanenbaum is the Practice Co-Chair of Polsinelli's Health Care Technology & Innovation Group, which is the second largest of its type according to the American Health Lawyers Association. Bill is the past President of the International Technology Law Association and was named by his peers as "Lawyer of the Year" in IT in New York in research by *US News & World Report*. He is the only lawyer ranked in Technology in the US and Global editions of *Chambers* whose practice focuses on healthcare. *Who's Who Legal* says he is a "well-known and highly respected practitioner" who has "expertise in technology transactions that puts him at the very top of the market", and that he is a "go to expert" on "the management and protection of data". *Chambers* finds that he "brings extremely high integrity, a deep intellect, fearlessness and a practical, real-world mindset to every problem".

Polsinelli
600 Third Avenue
42nd Floor
New York, NY 10016
USA

Tel: +1 212 413 2840
Email: wtanenbaum@polsinelli.com
URL: www.polsinelli.com

Polsinelli PC is a full-service AmLaw 100 firm with 900 lawyers in 21 cities in the United States. Its Health Care Department is one of the largest in the nation and its Health Care Technology & Innovation Group is the second-largest healthcare IT practice, both according to the American Health Lawyers Association. *US News & World Report* recognised the Health Care Department as a National Tier One practice for the last seven years and ranked Polsinelli as the "Law Firm of the Year" in healthcare. The firm also has a healthcare consulting firm, Polsinelli Health Care Solutions. The Technology Transaction & Data Privacy Group, which provides cross-disciplinary services with the Health Department, also received a National Tier One ranking. BTI Consulting ranks the Health Department in the top 3% in client relations and Polsinelli as one of the Top 30 firms in the US for client service.

www.polsinelli.com

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Artificial Intelligence and Cybersecurity in Digital Healthcare


James Devaney


Sonali Gunawardhana


Lischen Reeves


Jen Schroeder

Shook, Hardy & Bacon L.L.P.

Introduction

Digital health technologies provide new opportunities for preventing, diagnosing and managing life-threatening diseases and chronic conditions outside of traditional care settings, while empowering consumers to make better-informed decisions about their own health. Artificial intelligence (AI), mobile health (mHealth), health information technology (IT), wearable devices, and telehealth and telemedicine have revolutionised healthcare, leading to improved clinical outcomes, reduced pharmaceutical and medical device costs, more efficient drug development and clinical testing, and analytics-based personalised medicine. At the same time, these new technologies have tested the limits of existing regulatory and legal frameworks. Understanding how to navigate the regulations, intellectual property strategies and privacy laws governing digital health will help companies, medical providers, patients, and other stakeholders change the healthcare landscape as we know it.

Regulatory

The Rapid Introduction of Artificial Intelligence in Digital Healthcare

The 21st Century Cures Act[1] was signed into law on 13 December 2016. The Cures Act was designed to help accelerate medical product development to bring new innovations and advances to patients who need them faster and more efficiently. More specifically, the Act exempted certain software products from the definition of "medical device", which in turn resulted in the Food and Drug Administration (FDA) reexamining how it reviews medical applications that utilise various types of software. As a result, the FDA is encouraging an environment of innovation as the agency understands that there has also been a large amount of investment by various healthcare organisations in the use of artificial intelligence.

Artificial intelligence (AI) is defined as the "capability of a machine to imitate intelligent human behaviour".[2] It is viewed by the scientific community as the science and engineering of creating an intelligent machine that can use various techniques to create intelligent behaviour. The FDA believes AI and machine learning technologies have the potential to transform healthcare by deriving new and important insights from the vast amount of data generated during the delivery of healthcare daily.[3] The FDA explains that AI algorithms are software that can learn from and act on data.[4] Healthcare professionals, patients and their families are increasingly embracing digital health technologies to inform everyday decisions, from tools that more easily report blood glucose levels to smart watches that can detect atrial fibrillation, all of which allow patients better control over managing their personal healthcare needs.

In healthcare, the impact of AI, through natural language processing (NLP) and machine learning (ML), appears to be transforming healthcare delivery each day with new and novel products that further assist in the detection and treatment of various diseases. As is the case in other industries, it is expected that these technologies will continue to advance at a rapid pace over the next several years. The future of AI in healthcare could include tasks that range from simple to complex – from facilitating therapeutic drug and device design, reading radiology images, making clinical diagnoses and recommending treatment plans, all of which fall squarely under FDA oversight. The agency is taking a proactive stance on how best to ensure these products reach the market with appropriate safeguards.[5] Understanding how the FDA intends to regulate these products moving forward is paramount to successfully navigating the regulatory landscape that will be in place for the full lifecycle of the product.

Navigating FDA Guidance and Proposed Regulatory Review Pathways for Digital Health Products

Many medical devices now have the ability to connect to and communicate with other devices or systems. Devices that are already FDA approved, authorised, or cleared are being updated to add digital features, hence there is a need to reevaluate the regulatory pathway for these products given their new capabilities.

Because the current statutes and regulations were drafted before these technological advances, the FDA's regulatory landscape tends to be outdated when it applies to digital health. Given this outdated regulatory scheme, it sometimes can be a challenge for new players who have entered the app market, including medical device companies who are developing an app or an algorithm to help diagnose a disease or condition and pharmaceutical companies who are developing an app to support the use of an approved pharmaceutical drug. The FDA continues to work with the industry to develop guardrails around the various proposed regulatory review pathways, though there continues to be significant uncertainty with regard to what the FDA review pathway will look like in the future as it pertains to digital health.

The FDA's Digital Health Innovation Action Plan[6] outlines the agency's efforts to reimagine the regulatory review pathway to ensure patients have timely access to high-quality, safe, and effective digital health products. As a result of this plan, the FDA has been working on a Digital Health Software Pre-Certification program,[7] though it remains a concept as it has not been formally adopted as the way that certain digital health technologies will

© Published and reproduced with kind permission by Global Legal Group Ltd, London

be regulated in the future. The FDA is still in the process of determining whether this proposed regulatory pathway is appropriate in terms of its overall success as it applies to both efficacy and safety. If the FDA determines that this regulatory pathway is appropriate for digital health products, the question remains as to whether the FDA has the authority to implement this program without legislation from Congress. In addition to developing the Pre-Certification Program, the FDA also issued a final guidance titled, "Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act", in order to modernise its policies regarding digital health.

Acknowledging that in certain instances these AI-derived algorithms have demonstrated accuracy greater than that of a clinician, the FDA has approved several new medical technology products. There are also cases in which these technologies can further aid the clinician in determining the most appropriate course of treatment with even more accuracy, hence the FDA's desire to adopt a regulatory framework that is better suited to address these technologies in real time rather than continue to review these novel products utilising an outdated regulatory pathway.

To this end, the FDA released a new set of guidance documents in September 2019 to clarify its stance on regulating clinical decision support (CDS) tools,[8] including AI-driven and mobile health software that assist medical professionals in diagnosing and treating patients. The agency described a risk-based enforcement strategy to oversee software targeted at critical or severe medical conditions as well as machine learning algorithms that do not transparently detail the process of deriving a conclusion. This means an AI algorithm which predicts the likelihood of a patient suffering from a particular medical episode, or a learning algorithm that sifts through individuals at the population level in order to identify who is more at risk of a health condition, will most likely need to adhere to more stringent regulatory oversight. In order to navigate the current regulatory landscape, until alternative review pathways are adopted and fully implemented for digital health products, it is imperative to understand the regulatory pathways available and which one is best suited to your digital health product. Many of these review pathways are setting the basis for the proposed pathways; therefore, fully understanding the *de novo* classification request and 510(k) premarket submission process can only assist in navigating the regulatory framework.

Cybersecurity Concerns

Cybersecurity threats have become synonymous with the digital age and have become an issue that is important to private and government organisations, as well as consumers and patients worldwide. With numerous data breaches publicly reported across a multitude of industries including healthcare, many organisations have invested significant resources into combatting the risks presented by digital threats, including the FDA. The expanded connectivity of medical devices has led to improvements in patient care and greater efficiencies in the healthcare system but also presents cybersecurity risks that must be addressed to ensure such products are safe for patient use. Any time a medical device has software and relies on a wireless or wired connection, it may become vulnerable to cyber threats, especially if the device is older and was not developed with cybersecurity in mind.

Unfortunately, threats and vulnerabilities cannot be eliminated and reducing security risks can be challenging for all stakeholders along the product development and deployment chain. The healthcare environment is clearly multifaceted; therefore, it is imperative that medical device manufacturers, hospitals, and facilities work together to manage security risks. Many medical device manufacturers are now grappling with how best to ensure their devices are used solely for their intended use to care for patients and prevent harm by those with unscrupulous intentions. The FDA, along with the Federal Communications Commission, U.S. Department of Homeland Security, and U.S. Department of Commerce, are working together to develop a risk-based framework[9] that relies on the varied stakeholders working together towards a goal of trust and transparency.

In the interim, the FDA has provided guidance[10] to help manufacturers design and maintain products that are cyber secure. As technology continues to evolve, cybersecurity concerns will continue to be an area where vigilance and partnership with all the players in the healthcare area will determine overall success. Understanding who you need to partner with in order to reduce your cybersecurity risk is an ever-changing landscape and one where seeking expertise in intellectual property and privacy issues will allow for comprehensive understanding of overall responsibilities, thereby reducing overall risks.

Intellectual Property

New Opportunities Attract Tech Companies to Healthcare

Artificial intelligence (AI) is transforming healthcare by creating new opportunities and bringing new competitors to the industry. Among these are the technology companies that develop and leverage the AI underlying digital healthcare. And although they are non-traditional players in the healthcare industry, tech companies are rapidly innovating in this space. For example, Google recently developed an AI tool for early breast cancer detection,[11] and the Apple Watch® uses AI to detect an irregular heartbeat.[12] Furthermore, tech companies are increasingly filing for patents around their healthcare innovations. In fact, they constitute some of the largest patent filers in digital health.

Companies investing significant resources in digital healthcare must implement comprehensive business and legal strategies to capture and protect their resulting innovations. Such strategies should account for considerations that are unique to AI technology, several of which are discussed below. Tech companies are likely to have an advantage over traditional healthcare companies in this respect, because their existing intellectual property strategies may have been developed with AI considerations in mind. Meanwhile, traditional healthcare companies may need to adapt their existing intellectual property strategies in order to remain competitive in the digital healthcare space.

A robust intellectual property strategy should account for the multifaceted nature of digital innovations, particularly those utilising AI. Digital innovations often have many different components or steps, each of which should be evaluated for protection. This is a departure from the "one patent to one product" mentality, which is especially common in the pharmaceutical industry. As an example, consider a new medical device with an improved smart sensor that uses AI to reduce measurement errors. The new medical device is an obvious candidate for intellectual property protection. A robust intellectual property strategy will further recognise that the smart sensor may find uses in other products and applications and should thus also be considered for intellectual property protection. In fact, sometimes the most valuable innovations are developed before an end product is even contemplated, let alone completed. For example, audio compression technology was developed to reduce the size of large audio files while still preserving reasonable fidelity and

© Published and reproduced with kind permission by Global Legal Group Ltd, London

minimising latency during playback. This technology paved the way for the multibillion-dollar industry that includes portable music players, such as the iPod®, and services for downloading and streaming music.

Different facets of an innovation may call for different types of intellectual property protection. An innovative, externally facing product or component, such as the smart sensor mentioned above, may be well suited for patent protection. Conversely, a component that is used exclusively internally within a company, such as AI model training procedures or proprietary data sets for training AI models, might be better suited for trade secret protection. A defensive publication strategy may be appropriate for an application developed using an off-the-shelf AI model and other generally known components and procedures.

Crafting a Multifaceted IP Strategy for Digital Health

As evidenced by the preceding example, a comprehensive intellectual property strategy in digital health should account for patents, trade secrets, and defensive publications.

Patents: Patenting offers a company advantages beyond exclusivity – precluding others from practising the patented invention for the life of the patent – including opportunities for cross-licensing to facilitate freedom to operate and public recognition as an innovator. However, a company needs a provident patenting strategy to secure valuable patents in AI and digital healthcare. In particular, in order to maximise patent value, the strategy should address a number of issues that are inherent to AI technology, including subject matter eligibility and infringement detectability.

Regarding subject matter eligibility, patent claims that are directed to nothing more than an abstract idea are not eligible for patent protection in the United States.[13] This restriction has created an increasingly complex legal landscape for computer-related innovations in recent years. In Europe, patent claims on digital inventions need to solve a technical problem in a new and inventive, technical manner.[14] AI inventions based on mathematical algorithms should be tied to computer hardware, or have a technical purpose or be tied to a technical application.[15] Navigating these landscapes requires strategically describing and claiming AI-related inventions in order to maximise the chances of withstanding legal scrutiny. Additionally, certain aspects of digital health innovations may be eligible for patent protection, while other aspects are not. Thus, obtaining patent protection for AI and other computer-related inventions requires careful consideration and selective pursuit of the aspects that are most likely to satisfy the subject matter eligibility requirements.

A patent strategy for AI innovations should also consider infringement detectability. Detection may be achieved by observation or analysis of the target technology, reverse engineering, product literature describing the target technology, and relevant regulatory disclosures. Many aspects of AI are hidden or otherwise difficult to observe, such as the particular configuration of the neurons in an artificial neural network or a machine-learning model that resides on a competitor's backend computer server. It is challenging to detect and enforce against infringement based on such hidden aspects, and patents directed to inventions having low detectability are often deemed less valuable. Therefore, ideally, a patent should cover the detectable aspects of an invention. If an innovation is completely hidden from the public and it is not subject to mandatory regulatory disclosures, then it may be better suited for protection as a trade secret.

In the digital health space, it is also important for a patent strategy to contemplate cross-licensing opportunities. Digital innovation is cumulative, with each improvement building on previous technology that is often patented. Consequently, a digital product may be at greater risk of patent infringement than products in other technology areas. Cross-licensing patents reduces this infringement risk and thus facilitates freedom to operate by providing a company with the ability to continue innovating and selling digital products in a particular technology area. Additionally, digital technology patents are more likely to be utilised for licensing than for litigation. There are many reasons for this, including the sheer number of patents that often cover any given digital technology, the cost of patent litigation, and the uncertainty that certain computer-related patent claims will successfully weather litigation. Obtaining multiple patents around a particular digital technology not only provides better protection, but it also increases opportunities for cross-licensing. Digital technology companies often acquire clusters of patents around their digital products, with each piece of a product considered for potential patenting.

Trade Secrets: A trade secret is information, including computer programs, algorithms, and devices, that has economic value by virtue of the fact that it is not generally known to others in the industry and that is subject to reasonable efforts to maintain its secrecy.[16] AI innovations are often well-suited for protection as trade secrets, because certain aspects are typically used exclusively internally within a company. For example, compilations of training data for AI algorithms and model training procedures are generally kept internal. Thus, digital healthcare companies should consider implementing a trade secret program to facilitate the identification and protection of trade secrets and to ensure that trade secret policies are implemented consistently.

Defensive Publication: A defensive publication strategy entails publishing details of an invention in order to block another party from patenting it. A defensive publication does not "protect" an innovation in the traditional sense of exclusivity, but instead ensures freedom to operate by precluding others from obtaining exclusivity. A defensive publication strategy may be appropriate when uncertainty exists about the novelty of an invention (e.g. an application using known components like open source AI libraries and publicly available data sources, or an application using AI algorithms in known ways), or when a company does not want to invest in patenting because infringement would be difficult to detect or the relevant product is not a source of significant revenue. In order to be effective, a defensive publication should be comprehensive and technically robust. It should include technical details, such as code and a description of the AI algorithm or model training, as well as a description of the digital healthcare product, how it is made, and how it could be used in a clinical setting.

In addition to the multi-pronged approach to intellectual property protection discussed above, a company's strategy around digital healthcare innovation should also account for the use of open source software. Due to the complexity of AI technology, many developers rely on open source software libraries to construct AI products. Open source code for many types of AI models and algorithms is free and widely available. In very little time, a researcher or software developer can choose an AI model type, configure its hyperparameters, train, validate, and then deploy an AI algorithm in an application. The open source code is typically copyright-protected under a licensing scheme that imposes certain obligations on developers who use the code. Often under these schemes, if a company releases a digital product that was developed using open source code, the company may be required to make the source code for their product freely available, identify the modifications made to the underlying open source code, and provide a copy of the applicable license. Licensing terms may also prohibit patenting

© Published and reproduced with kind permission by Global Legal Group Ltd, London

technology that is implemented using open source code. Accordingly, companies must carefully consider their intellectual property strategy in scenarios involving open source code. For instance, a company may want to implement restrictions on releasing digital products that use open source code or consider a defensive publication strategy for digital products that use open source code.

Finally, a company's intellectual property strategy should contemplate scenarios of collaborative innovation and intellectual property created in the employment context. Increasingly, traditional healthcare companies are collaborating with technology companies to develop AI and digital healthcare products. A healthcare company may hire technology consultants and vendors to assist with such development. The healthcare company may assume that it automatically owns the intellectual property created by the people working for the company, but this assumption is wrong and can lead to disastrous consequences for the company. In order to ensure ownership and control of this intellectual property, it is critical for the healthcare company to require all individuals performing work for the company, including its employees, independent contractors, and consultants, to sign agreements that include assignment and confidentiality provisions. Ideally, these agreements should be executed before work commences in order to ensure that all parties are in agreement regarding intellectual property ownership before the intellectual property is created, as well as to ensure the agreement is supported by valid consideration.

Privacy

Rethinking Privacy and Security Compliance in the Digital Health Era

The longstanding standard in healthcare privacy and security compliance is the Health Insurance Portability and Accountability Act (HIPAA), which Congress enacted in 1996. HIPAA requires "covered entities" and their "business associates" to protect against wrongful access, use, disclosure, and transmission of patients' Protected Health Information (PHI).[17] The Health Information Technology for Economic and Clinical Health (HITECH) Act amended HIPAA in 2009 by further solidifying security measures, especially in regard to electronic PHI (ePHI). The HIPAA Privacy and Security Rules guide covered entities in protecting the integrity and confidentiality of PHI and ePHI. While HIPAA's protective reach is admirable, the law predates new and exceptional technological growth and innovation in healthcare. For this reason, HIPAA increasingly represents only a baseline – albeit an ever important one – of security protocol for covered entities and business associates in this new era of digitalised healthcare. In some instances, with the rise of the Internet of Medical Things (IoT) – e.g. wearables, sensors, mobile applications, etc. – many digitalised healthcare innovators are operating outside of HIPAA's protective barriers thereby requiring privacy and security guidance under the California Consumer Privacy Act (CCPA) or General Data Protection Regulation (GDPR), whichever is applicable. In any event, a new approach to healthcare cybersecurity is warranted – if only to rebuild patients' and consumers' trust in the industry. This new approach would entail petitioning Congress to modernise HIPAA by refreshing critical definitions, and assisting companies handling PHI but not subjected to HIPAA with building strong cybersecurity strategies and cultures under CCPA or GDPR.

The following are three reasons to rethink privacy and security in the digitalised healthcare era:

- HIPAA's focus is narrow.
- The healthcare industry is particularly vulnerable to ransomware attacks.
- Cybersecurity requires much more than rules-based compliance.

HIPAA's Narrowed Focus

HIPAA regulates healthcare data custodians, rather than healthcare data. Only a certain group of entities – e.g. hospitals, physicians, insurance providers – are subjected to HIPAA's rules.[18] The gap in healthcare data protection occurs when major technological players like Amazon, Apple, Google, and Facebook enter the healthcare industry by adding to the IoT, which consists of wearables, sensors, and mobile applications, and increasing the use of artificial intelligence to diagnose and treat health-related issues.[19] These entities are not your typical "covered entities". Therefore, the healthcare data accessed, used, disclosed, or transmitted from their various platforms operate outside of what is referred to as the HIPAA-zone.[20]

Because most innovations that make up the IoT allow companies to deal directly with the patient and exclude the healthcare entity, there is an audible sigh at the recognition that HIPAA may not apply.[21] However, even where an entity dodges HIPAA compliance, other governing rules and regulations might still be in effect. One example is the California Consumer Privacy Act (CCPA). The CCPA is not tied to regulating HIPAA-covered entities. In fact, it includes a HIPAA carve out by stating the following:

This title shall not apply to any of the following: "... (B) ... a covered entity governed by [HIPAA] ... to the extent the ... covered entity maintains patient information in the same manner as ... [PHI]".[22]

The CCPA essentially begins where HIPAA ends. It is applicable to *all* entities that handle healthcare data, therefore filling the gap. This is helpful guidance for an industry in desperate need of regaining its consumers' trust by drastically increasing cybersecurity measures beyond HIPAA compliance.[23]

Ransomware Attacks are on the Rise

The HIPAA Security rule requires covered entities to create and implement administrative, technical, and physical safeguards to protect the integrity and confidentiality of ePHI. But technical safeguards, even for entities not regulated by HIPAA, can be difficult to implement, which is why we see a rise in ransomware attacks in healthcare, including attacks on medical devices.[24] The Department of Health and Human Services (HHS) defines ransomware as:

> ...a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.[25]

The healthcare industry is more likely to sustain ransomware attacks and other data attacks than any other industry.[26] In 2015 alone, 100 million healthcare records were compromised. Within the last few years, over 90% of healthcare entities have reported a data breach.[27] While HIPAA's Security Rule

© Published and reproduced with kind permission by Global Legal Group Ltd, London

calls for a risk analysis[28] and subsequent development of risk management processes and protocols aimed at exposing security vulnerabilities, even HHS had to admit HIPAA does not include a standard that "specifically and expressly requires entities to update the firmware of network devices".[29] This means that even a robust HIPAA compliance strategy may still leave covered entities and their business associates vulnerable.

Rules-based Compliance is Insufficient

What might assist cybersecurity in the digitalised healthcare era is risk management tailored to mitigating unpredictable attacks. Harvard Business School professors Robert Kaplan and Annette Mikes write that the best preparation for external, unpredictable risks is a company culture enthused with discussion, and not only rules-based compliance.[30] HIPAA, as it currently stands, is rules-based and protects against predictable attacks. While this is necessary, it is not enough. Criminal hackers do not announce their arrival, and they come to disrupt in unpredictable ways. More conversations amongst everyone in the organisation (not only legal and compliance personnel, but also top-level executives) about the wide-ranging threats healthcare data faces will lead to establishing a security-minded organisation and comprehensive breach response plans crucial to warding off unpredictable and creative attacks.

Recommendations and Solutions

Modernise HIPAA: Congress should do the following to increase HIPAA effectiveness:

1. Expand the definition of "covered entity". The digitalised health era requires a reasonable addition of entities set on disrupting the healthcare industry.
2. Focus on data protection rather than custodian regulation. All individually identifiable healthcare data should be protected, regardless of the nature of the entity handling the data.

Create a Security Focused Culture under CCPA or GDPR: Companies operating outside of the HIPAA-zone can position themselves as consumer and data security focused by implementing CCPA and GDPR guidance critical to healthcare data including the following:

1. The CCPA and GDPR's "right to forget" clauses. With certain exceptions, the clauses require that data handlers delete PHI a consumer provides at that consumer's request.[31]
2. The GDPR and CCPA's standards on third-party risk management. These provide more details than HIPAA's.[32]

[This section was prepared with input from Shook Privacy & Data Security Practice Chair, Al Saikali.]

Conclusion

Digital health technology continues to expand though there are factors that must be addressed. Some of these factors include the following: regulatory pathway uncertainty; financial constraints, including appropriately allocating intellectual property rights; continued concerns regarding ensuring patient confidentiality/privacy; and lack of interoperability between healthcare systems, as well as cybersecurity concerns. Understanding how to address the changing legal landscape will encourage innovation in the ever-changing field of digital health while also protecting the world's public health.

Endnotes

1. Pub. L. 114–255.
2. Definition from Merriam-Webster Dictionary. *See*: https://www.merriamwebster.com/dictionary/artificial%20intelligence.
3. Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning Based Software as a Medical Device, Discussion Paper.
4. https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.
5. https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.
6. *See* https://www.fda.gov/media/106331/download.
7. https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program.
8. https://www.fda.gov/media/109618/download.
9. https://www.fda.gov/medical-devices/digital-health/health-it-risk-based-framework.
10. https://www.fda.gov/medical-devices/digital-health/guidances-digital-health-content.
11. *Google's AI breast cancer screening tool is learning to generalize across countries*, MIT Technology Review, https://www.technologyreview.com/f/615004/googles-ai-breast-cancer-screening-tool-is-learning-to-generalize-across-countries (3 January 2020).
12. Steve Dent, *AI-equipped Apple Watch can detect the signs of a stroke*, Engadget, https://www.engadget.com/2017/05/12/ai-equipped-apple-watch-can-detect-the-signs-of-a-stroke (12 May 2017).
13. *See* 35 U.S.C. § 101; *Alice Corp. v. CLS Bank Intl'l*, 134 S. Ct. 2347, 2355 (2014) (citing *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66, 70–73 (2012)) (creating a two-stage framework that is used to determine whether claims are eligible for patent protection).
14. *See* European Patent Office Guidelines for Examination of Programs for Computers G-II, 3.6; Guidelines for Mathematical Methods G-II, 3.3 and for Artificial Intelligence and Machine Learning C-II, 3.3.1.
15. *Id.*
16. Uniform Trade Secrets Act § 1(4) ("'Trade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.").
17. *See* 45 C.F.R. § 160 *et seq.*
18. *See* 45 C.F.R. § 160 *et seq.*
19. https://aabme.asme.org/posts/internet-of-medical-things-revolutionizing-healthcare.
20. Nicholas P. Terry, Regulatory Disruption and Arbitrage in Healthcare Data Protection, 17 YALE J. HEALTH POL'Y L. & ETHICS 143 (2016).
21. *Id.*
22. Cal. Civ. Code § 1798.145(c)(1)(B).
23. Sateyender Goel, *California Consumer Privacy Act and the Future of the Health Data Economy* (7 November 2019), https://medcitynews.com/2019/11/california-consumer-privacy-act-and-the-future-of-the-health-data-economy.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

24. Lily Hay Newman, *Medical Devices Are the Next Security Nightmare,* WIRED (2 March 2017), https://www.wired.com/2017/03/medical-devices-next-security-nightmare.
25. U.S. DEP'T. OF HEALTH & HUMAN SERVS., FACT SHEET: RANSOMWARE AND HIPAA (2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf [http://perma.cc/AS48-JNRP].
26. Cybersecurity in the Healthcare Industry, INFOSEC INSTITUTE (23 May 2016), http://resources.infosecinstitute.com/cybersecurity-in-the-healthcare-industry/ [https://perma.cc/B67V-J5Z9].
27. Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security*, Rule and NIST Cybersecurity Framework,* U.S. DEP'T. OF HEALTH & HUMAN SERVS. (23 February 2016), http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/[https://perma.cc/MZV3-RAXM].
28. The Office of Civil Rights ("OCR") Guidance on Risk Analysis Requirement under the HIPAA Security Rule (14 July 2010), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.
29. *Id.*
30. Managing Risks: A New Framework, Harvard Business Review (June 2012), https://hbr.org/2012/06/managing-risks-a-new-framework.
31. *See* GDPR Art. 17; Cal. Civ. Code. § 1798.105(a).
32. *See* GDPR Art. 28, 32; Cal. Civ. Code § 1798 *et seq.*

© Published and reproduced with kind permission by Global Legal Group Ltd, London

James Devaney is a partner in Shook's Intellectual Property Group. His practice focuses on strategic IP counselling to help companies acquire, protect and monetise IP and reduce exposure. He has more than 15 years of experience leading patent due diligence for a wide range of transactions, evaluating strategic acquisitions, and conducting patent portfolio analyses. He manages legal and technical teams, works closely with product developers to implement patent design-around solutions, and creates patent strategies aligned with business objectives. James is an adjunct law professor and has drafted hundreds of patent applications for artificial intelligence and machine learning innovations in digital healthcare and computer technologies.

Shook, Hardy & Bacon L.L.P.
2555 Grand Blvd.
Kansas City, MO 64108
United States

Tel: +1 816 559 2677
Email: jdevaney@shb.com
URL: www.shb.com

Sonali Gunawardhana draws on her nearly 10 years' experience as an attorney at the U.S. Food and Drug Administration (FDA) to offer clients detailed and practical guidance on how to avoid and resolve FDA regulatory challenges. Her practice focuses on FDA regulatory requirements for bringing medical devices and pharmaceuticals to market as well as how best to navigate post-approval regulatory requirements. Sonali assists both medical device and pharmaceutical companies to determine the best regulatory pathway in which to seek approval for their digital health products.

Shook, Hardy & Bacon L.L.P.
1800 K St. NW, Suite 1000
Washington, D.C. 20006
United States

Tel: +1 202 639 5643
Email: sgunawardhana@shb.com
URL: www.shb.com

Lischen Reeves focuses her practice in data privacy and security matters, and national business and employment litigation. Her work is concentrated in providing guidance and litigation expertise to healthcare entities under the Health Insurance Portability and Accountability Act, as well other state data privacy and security laws. She is also a member of Shook's biometric privacy practice and defends corporate employers in a variety of commercial and employment-related disputes. Lischen is often engaged in early litigation risk assessment, pretrial work, discovery, legal analyses and mediation statements.

Shook, Hardy & Bacon L.L.P.
2555 Grand Blvd.
Kansas City, MO 64108
United States

Tel: +1 816 559 2056
Email: lreeves@shb.com
URL: www.shb.com

Jen Schroeder counsels clients on patent, trademark, copyright, trade secret and general intellectual property matters. She performs strategic IP portfolio analyses, provides patentability and freedom to operate opinions, conducts IP due diligence, evaluates patent cross-licensing and monetisation opportunities, and counsels clients with respect to licensing, acquisition and confidentiality agreements. She also works on post-grant proceedings, including *inter partes* review proceedings. Her patent procurement practice includes preparing and prosecuting U.S. and international patent applications in various technologies including computer software, medical devices, telecommunications, and chemical and mechanical arts.

Shook, Hardy & Bacon L.L.P.
2555 Grand Blvd.
Kansas City, MO 64108
United States

Tel: +1 816 559 0314
Email: jschroeder@shb.com
URL: www.shb.com

With a well-earned reputation as a litigation powerhouse, Shook, Hardy & Bacon is the go-to firm for the world's leading health, science and technology companies. Shook advises multinational pharmaceutical and medical device, technology and R&D companies on the intellectual property and privacy implications of digital health services, including cybersecurity, artificial intelligence, and blockchain. Shook also advises clients on various regulatory issues, offering a comprehensive perspective on the possibilities and potential risks of digital health. Shook's multidisciplinary teams include not only former FDA, FTC and SEC lawyers but certified IAPP fellows and attorneys with backgrounds in healthcare, life sciences, software and computer engineering, many of whom have scientific and technical degrees. Founded in 1889, Shook has 15 offices in the United States and London, with approximately 500 attorneys in areas ranging from IP and product liability to commercial litigation and environmental/toxic tort. To learn more, explore Shook's Digital Health Practice here: https://www.shb.com/services/industries/digital-health.

www.shb.com

SHOOK
HARDY & BACON

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Privacy in Health and Wellbeing


Marta Dunphy-Moriel


Hayley Davis


Glafkos Tombolis


Aneka Chapaneri

Kemp Little LLP

Part 1: Setting the Scene

1 Overview of current state of the digitalisation of health and wellbeing. Drawing the line between a wellbeing device and a medical device

There is no doubt that healthcare and wellbeing is becoming increasingly digitalised and there are manifold reasons for this.

First, healthcare systems in the western world (particularly those that are taxpayer-funded, such as the UK's National Health Service) are under increasing pressure to deliver better health outcomes and reduce the cost of delivery – this has resulted in increasing adoption of digital infrastructure and assets, ranging from the collation, processing and extrapolation of patient medical data, to the benchmarking of costs to optimise organisational efficiencies.

Second, and perhaps as a consequence of the strain on public healthcare systems, employers in the private sector are assuming increasing responsibility for healthcare provision. Clearly, any investment in technology by private businesses needs to generate a minimum return on investment; the payback for employers in healthcare and wellness technology investment is increased employee productivity, and hence, profitability.

Third, and again as a result of the increasing burdens placed on public healthcare systems, there has been an increase in the provision and sophistication of private healthcare insurance products. This has inevitably resulted in greater digitalisation, since a data-driven approach to assessing health-related risks leads to better underwriting decisions.

Finally, no doubt thanks to social media penetration, Digital Health is becoming more high-profile; there has been a proliferation of consumer-focussed devices such as applications and associated wearables used to monitor fitness, wellness and other medical or healthcare requirements.

Global investment in the Digital Health market has been rapidly increasing over the past five or so years, with major technological developments for the public and private sectors alike. This increased investment has been triggered by growing pressure on healthcare providers caused by the effects of an ageing population and a greater awareness and interest from general consumers about their mental and physical health and wellbeing. With major technology suppliers and healthcare providers investing heavily to boost their Digital Health offerings, financial predictions suggest that the current momentum is only likely to accelerate further over the foreseeable future.

Nearly all Digital Health offerings will involve collecting, producing and accessing data, including personal data and, given the nature of the offerings, this will often include special categories of personal data such as health information, genetic or biometric data. Many Digital Health offerings will also require the sharing of data with other suppliers, organisations and healthcare professionals. Therefore, compliance with applicable data protection legislation and data security requirements in all relevant jurisdictions will be vital, particularly when commercialising the data.

2 Distinctions between a wellbeing device and a medical device

The recent boom in health and wellbeing advancements by technology suppliers that do not traditionally operate in the medical sector has prompted additional guidance from regulators (such as the European Medicines Agency ("**EMA**"), the UK Medicines and Healthcare products Regulatory Agency ("**MHRA**") and the U.S. Food and Drug Administration ("**FDA**")), in order to help suppliers creating wellness products, devices and applications and to understand when their respective products, devices or applications cross into the scope of a regulated medical device.

Medical devices are highly regulated in the European Union ("**EU**") and have to undergo a conformity assessment to demonstrate that they meet the necessary legal requirements to ensure they are safe and perform as intended. The conformity assessment process is dependent on the categorisation of their medical device,[1] but can be a protracted process, and usually involves an audit of the manufacturer's quality system and, depending on the type of device, a review of the technical documentation from the manufacturer on the safety and performance of the device. Manufacturers will need to determine the categorisation of their medical device to determine the relevant route to compliance.

In summary, in the UK, a device will be considered a medical device if it falls within the scope of the definition. In the UK, we are currently mid-way through a transition period moving over from the older legislation under the UK Medical Devices Regulations 2002 ("**UK MDR**") to the newer Medical Device Regulation[2] ("**MDR**") and the *In Vitro* Diagnostic Medical Devices Regulation[3] ("**IVDR**"). During the transition period, manufacturers can place devices on the market under the UK MDR or the MDR/IVDR if they fully comply with the relevant requirements.

Under the UK MDR, a medical device includes any instruments or other articles that: (a) are intended to be used to diagnose, prevent, monitor or treat disease or an injury, or to investigate or modify the anatomy or a physiological process, or to control conception; and (b) do not principally work by a physiological function, by pharmacological, immunological or metabolic

© Published and reproduced with kind permission by Global Legal Group Ltd, London

action (as devices that principally work by a physiological function, by pharmacological, immunological or metabolic action are regulated under separate medicines regulations).

However, wellbeing devices are only intended to be used in the monitoring of general fitness, general health and general wellbeing or to promote a healthy lifestyle, and therefore present minimal risk to the health and safety of the user and others. As a result, wellbeing devices are subject to little or no specific medical regulatory requirements, dependent on where the device is used and the type and function of the device.

Part 2: Key Privacy Challenges

1 Privacy in health

Privacy compliance has become a key priority of all companies for many reasons. Aside from the obvious point of their legal obligations and the risk of fines, the potential reputational damages and loss of user trust encourage companies to take privacy very seriously. Privacy in healthcare has additional challenges as the companies in this sector are in a vital position as they process the full spectrum of data, from financial records and health insurance information to patient test results and biometric information. Because of the volume of sensitive data processed by stakeholders operating in this space and the massive impact that a privacy issue could cause to patients, the business and the advancement of science make privacy compliance a particularly complex issue.

(a) Privacy in clinical trials

Whether you are a Sponsor or a clinical site performing trials on healthy or sick patients, privacy plays a key role in the clinical trial process.

Where privacy comes in

There are three aspects of the clinical trial process where privacy plays a key role:

- The Clinical Trial Protocol ("**Protocol**"):
  As part of the Protocol, Sponsors must include measures that ensure that (i) only the necessary personal data is collected, and (ii) that the researchers and clinical sites are given clear instructions about what personal data is collected and how it is processed as part of the clinical trial. Most trials are likely to fall into the general requirement to carry out a Data Protection Impact Assessment ("**DPIA**").[4] Even if a DPIA is not legally required, it is always advisable to carry out a DPIA in a clinical trial context to better understand and justify the processing. A DPIA is also a useful tool to identify what privacy items need to be included in the Protocol.
- The Clinical Trial Agreement ("**CTA**"):
  It is essential that the CTA includes the necessary privacy wording to regulate how clinical sites and researchers will process personal data.
  In our experience, Sponsors will face two key challenges on the CTA front:
  i. **Standard CTAs:**
  Regulator-issued template CTAs issued by the local authorities may not yet include privacy language. It is likely clinical sites and ethics committees alike will be resistant to allowing privacy amendments to the standard documents. This means that (i) privacy issues may not be covered by the CTA, and (ii) the ethics committee may refuse to permit a separate processing agreement to be signed (as all the terms governing the clinical trial must be in the CTA).

ii. **Controller *vs* Processor**:
The crux of the issue is who has control and overview of the processing activities. Whereas there is consensus that contract research organisations ("**CROs**") are always processors on behalf of the Sponsor, in the case of clinical sites it is not so clear cut.
If the clinical site is a processor, it will only process the personal data as per the Sponsor's instructions which, in practice, means that they will only use personal data as per the Protocol. In this context, the Sponsor will have complete oversight of any processing that is being carried out in this context. Whereas in theory this seems the most practical solution and would only require adding processing wording,[5] most clinical sites are reluctant to take on a processor role.
There are several reasons why clinical sites would rather be a controller, some of which we mention for reference below.

- **Ownership of data**: There is widespread confusion between controllership in a privacy sense and ownership in an intellectual property ("**IP**") sense. Contrary to popular belief, in our view it is very unlikely that the fact that a clinical site is a controller of clinical trial personal data would grant them additional IP rights over the personal data. The clinical site's role as controller would not, initially, overlap any restrictions established in the IP terms of the CTA.
- **Overlap**: The most common reason is that a lot of the personal data that is collected for the clinical trial is already in the clinical site's possession and it needs to be used for the clinical site's own purposes (for example, treating the patient). This means that the sites will be concerned that they will not be able to comply with many of the controller's instructions as a processor (such as deleting data on termination) which would put them in breach of the CTA.
- **Reporting obligations**: Most clinical sites find that processor notification obligations are too complicated to carry out efficiently in practice. There are several reasons for this, including the fact that the lines between what they do as separate controllers (i.e. treating patients), and what they do on behalf of the Sponsor, are in many cases blurred. Also, the PR impact and loss of trust is a risk that needs to be managed cautiously. Moreover, it does not help that many clinical sites are not legally sophisticated and are often understaffed.
- **Flow-down of specific policies and procedures**: The bureaucratic burden of a heavily regulated clinical site is substantial and difficult to amend, both in practice but also due to internal resistance. Clinical sites therefore want as much autonomy as possible regarding how they comply with their legal obligations.
- **Holding the keys to de-pseudonymise**: Clinical Trial Regulations[6] ("**CTR**") require Sponsors to only receive pseudonymised data which, prior to the General Data Protection Act ("**GDPR**") was considered "anonymous" by the pharmaceutical industry). Any identification of a patient can render trial data unusable and, in an extreme case, jeopardise the trial. Therefore, it is crucial that clinical sites only provide pseudonymised data to the Sponsor. This means that

© Published and reproduced with kind permission by Global Legal Group Ltd, London

the party that holds the keys to de-pseudonymise the data is the clinical site: this provides strong decision power over the personal data that gives clinical sites an argument towards controllership. However, the counter argument is that this proves that the clinical site is a processor because the site only pseudonymises the data because the Sponsor is instructing it to do so.

- **Data sharing between controllers does not require mandatory contractual wording:** This means that the clinical site need only sign (and, to the extent applicable, negotiate) the CTA. Clinical sites consider this to be more practical as the site can decide how it complies with its privacy obligations, without having to undertake additional contractual commitments.
- **Sub-processors:** As an independent controller, the clinical site is not subject to the general veto rights of the Sponsors regarding any sub-processors it needs to engage.

- The Informed Consent Form ("**ICF**"):
  The ICF must be:
  i. worded such that it can be read and understood by people who are not healthcare professionals, who have not received verbal information and which potential participants may wish to consult;
  ii. written in a language that is clear and understandable for the participant. It must also include all fair notice requirements;[7] and
  iii. a short single document.
  The requirement is simple; the practicality of drafting an ICF unfortunately is not. Sponsors will need to balance both requirements on a case-by-case basis. It is vital that Sponsors tailor the content to their specific patient pool and consider cultural sensitivities, especially if the ICF is addressed to non-healthy patients.

(b) Sharing patient data

Sending personal data to regulators

If a controller is required to share special category data, such as health data, under the GDPR, it must identify a lawful basis for sharing and an additional special condition.[8]

In the context of safety reporting or an inspection by a national competent authority, the processing, and therefore sharing, of personal data has to be considered as necessary to comply with the legal obligations that the Sponsor and/or the investigator is subject to. Therefore, the appropriate condition for the processing of patient data in this context will be processing what is necessary for "reasons of public interest in the area of public health".[9]

Sharing with other Sponsors/selling results

Whereas sharing aggregated data is generally out of scope of the GDPR, Sponsors must carefully review the parameters to ensure that the data is irreversibly anonymised. In some cases, the parameters of the study are so narrow that it is impossible to consider the data anonymous. This is a common occurrence, for example, in rare disease trials.

The European Data Protection Supervisor ("**EDPS**") has stated in its first 2020 Opinion[10] that it encourages data sharing for the purpose of scientific research and is due to issue further guidance on this point.

(c) Legal basis for processing

The European Data Protection Board (**EDPB**) distinguishes[11] the two main categories of processing activities relating to a specific clinical trial protocol during its whole lifecycle as:

- Reliability and safety related purposes
  For processing activities in relation to reliability and safety purposes as stated in the CTR and national laws, the EDPB is of the opinion that the most appropriate lawful basis for processing personal data is the "legal obligation(s) to which the controller is subject".[12] Similarly, the appropriate condition for processing special category data in this context is "necessary for the reasons of public interest in the area of public health…".[13] The EDPB considers that the types of processing activities that will fall under this category are safety reporting, inspection by a national competent authority or the retention of clinical trial data in accordance with archiving obligations under the CTR.
- Research activities
  For processing in relation to research activities, the EDPB considers that the appropriate lawful bases may be either:
  i. The data subject's explicit consent:[14]
  The guidance highlights the importance of not confusing the notion of "informed consent" under the CTR with the lawful basis of consent under the GDPR. Consent under the GDPR must meet the criteria specified in Article 7 GDPR, namely, the consent must be specific, informed, unambiguous and most importantly, freely given. In the context of special category data, such as health data, the individual's explicit consent should be obtained.[15] The EDPB states that when considering whether explicit consent is the most appropriate lawful basis for processing special category data in the context of a clinical trial, controllers should take into account the Working Party 29 ("**WP29**") guidelines on consent, and check if all the conditions for valid consent can be met. Importantly, consent will not be a valid lawful basis where there is a clear imbalance of power between the Sponsor/investigator and the participant. If consent is relied on, there must be a mechanism provided to enable individuals to withdraw that consent at any time.
  ii. A task carried out in the public interest or the legitimate interests of the controller:[16]
  The EDPB considers that the lawful basis of public interest may be more appropriate than the data subject's consent. The processing of personal data in the context of clinical trials may be considered as necessary for public interest reasons where the "conduct of the clinical trial directly falls within the mandate, missions and tasks vested in a public or private body by national law". For other situations which do not meet the public interest requirements, the processing may be necessary for the legitimate interests of the controller.

Secondary uses of clinical trial data for scientific purposes

The EDPB states that if a Sponsor or an investigator would like to further use the personal data gathered in a clinical trial outside of the remit of the clinical trial protocol for scientific purposes, another lawful basis will be required and the presumption of compatibility under Article 5(1)(b) GDPR will not apply.

Healthy vs non-healthy patient trials

It is important to understand the context of the trial before considering the most appropriate lawful basis as the participant's health and wellbeing may impact the availability of various lawful bases.

In the context of a trial where the patients are "healthy", there is a lower level of risk present when considering

© Published and reproduced with kind permission by Global Legal Group Ltd, London

consent as the most appropriate lawful basis. Under the GDPR, a key criterion of "consent" is that it must be "freely given". A healthy patient is likely to have the requisite capacity to be able to freely give their consent and to make an informed decision.

On the other hand, where patients cannot be considered as "healthy", the lawful basis of consent will not be the most appropriate and would not be considered valid without the criterion of being "freely given".

(d) Data subject right of access

Patients can access their data

The EDPS has warned that *"any derogation from these essential data subject rights must be subject to a particularly high level of scrutiny in line with the standards required by Article 52(1) of the Charter"*.[17] There are, however, some conditional exemptions to data subject rights for research purposes under the GDPR. The most important condition to the exemption is that complying with the data subject's rights request would "prevent or seriously impair the achievement of the research purpose". The UK Health Regulatory Authority ("**HRA**") guidance[18] highlights the importance of what the research participants have been told about their data subject rights and the withdrawal from the study.

The right of data subjects to access their personal data does not apply when data is processed for health or social care research purposes and where the following conditions have been satisfied:

i. appropriate safeguards are in place; and
ii. the results of the research or any statistics are not made available in a form which identifies the data subject or, in the opinion of an appropriate health professional, disclosure to the data subject is likely to cause serious harm.

Difficulties for Sponsors when dealing with access requests

The element on anonymity in clinical trials is fundamental to the research results collected by the Sponsors. It is crucial that a Sponsor does not receive a subject access request from a clinical trial participant directly, otherwise they will be forced to discard the data in relation to this participant. Sponsors must appoint an intermediary to act as a "post-box" in receiving the access requests from the participants and implement protocols to ensure that the intermediary pseudonymises the participant's personal data before sending it on to the Sponsor so that the Sponsor merely receives limited information, such as the participant's ID number. To prevent a clinical trial participant from submitting a subject access request directly to the Sponsor and therefore identifying themselves, Sponsors should ensure that alternative contact details are provided for the Sponsor's intermediary, such as an external data protection officer.

Deleting patient data

Under the GDPR, individuals are entitled to exercise their right of erasure, or more commonly known as the "right to be forgotten" in order to request that the organisation holding the individual's data deletes their personal data without undue delay. This right can prove difficult for Sponsors who require the data in order to provide valid results in the outcome of a clinical trial. However, there are various exemptions to the right of erasure under the GDPR, which Sponsors can seek to rely on in certain circumstances where the processing is necessary for:

i. Compliance with a legal obligation[19]
   This exemption may be relied on when the processing of participant personal data is necessary in order for the Sponsor to comply with its legal obligations under EU law. For example, this may include any obligations to retain clinical trial data for audit purposes. This does not mean, however, that clinical trial data may be retained forever; a clear retention period must be established and, where necessary, explained to the participant.[20]
ii. Scientific research purposes[21]
   This exemption may be relied on when the processing of participant personal data is necessary for scientific research purposes and if the request for erasure of participant data was exercised in this circumstance, this would "render impossible" or "seriously impair" the objective of the achievement of the clinical trial.

(e) A practical point

A Sponsor must obtain a positive opinion from a local ethics committee before commencing a clinical trial in the EU. Ethics committees are independent bodies with their primary responsibility being to ensure that the rights, safety and well-being of patients participating in clinical trials are met. When providing their opinion in relation to a Sponsor's clinical trial, the ethics committee should consider the adequacy and completeness of the written information that will be provided to the individuals participating in the trial (particularly, where the patients are considered as vulnerable individuals) and the procedure for obtaining these individuals' informed consent.

There is no identified harmonised approach between ethics committees or regulators within the EU, so Sponsors should be aware that their clinical trial documents may need to be localised in various jurisdictions.

2 Privacy in Digital Health

(a) Privacy and medical devices

Many medical devices use technology to assist with treatment, keep track of health metrics or even spot trends. Medical devices are increasingly used to make automatic decisions based on these patterns, with the aid of AI.

This data can be used both to treat the specific medical condition it has been collected to analyse and to improve the device itself. It is also possible for AI to spot unsuspected patterns (both in medical device data and historical data) that lead to the diagnosis and/or treatment of unrelated illnesses.

AI has the potential to benefit millions of people by revolutionising diagnostics and treatment. It is therefore crucial that companies strike the right balance between these benefits and patients' right to privacy. To the extent possible, companies should anonymise data[22] to enable data sharing and indefinite retention of the necessary data that will, with the help of AI, help get better diagnostics.

(b) Giving notice

Complying with transparency (and, if applicable, consent) obligations in a Digital Health context does not come without a challenge.

Determining who interacts with the individual

Whereas it is the controller's responsibility to comply with the transparency obligations under privacy laws, in practice, it is often that controllers of medical device data need to rely on the party providing the device to the patient to give notice and, where applicable, to obtain relevant consents.

Examples of direct interaction with the patient include providing information in the medical device screen, providing hard copies of documents with the medical device and requiring an app to use the device or requiring registering the medical device on a controller portal before use. If the controller has a direct means of communication with the patient, even if they

© Published and reproduced with kind permission by Global Legal Group Ltd, London

cannot put a name to a user, they have a sufficient level of interaction to give notice directly.

Relying on third parties

For controllers, this means that in many instances they must rely on a third party to obtain consent on their behalf, which will require strong contractual assurances and careful supervision that this is being done adequately.[23] If a controller relies on consent obtained by a third party, the controller must be specifically named in the consent request. Categories of third-party organisations in a consent request will not be enough to obtain valid consent under the GDPR.

Privacy by design by manufacturers

In most cases, medical device manufacturers will determine what data is collected. Whereas controllers can choose a specific device, in some cases there is a lack of choice as many devices are unique. It is therefore the manufacturer who needs to ensure that only data which is strictly necessary for the purpose is collected.

Moreover, if the device is online, the data is likely to be sent back to the provider (generally acting as a processor), normally in real time. It is therefore key that manufacturers ensure that the processes are designed to keep data safe both in the device itself but also during its transmission and subsequent processing in the provider's systems.

It is not uncommon, however, for medical devices not to be connected to the internet and still collect personal data. The personal data is then retrieved manually from the device by the provider and transported to their facilities for further processing. In this scenario, it is vital that measures are taken to ensure that the data that is collected manually is handled only by security trained authorised individuals and that any devices that are decommissioned are properly wiped of all data.

(c) Data subject rights

If the personal data processed by a controller does not permit the controller to identify a natural person, the controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of the GDPR.[24]

(d) Pseudonymisation and anonymisation

Personal data will be considered "pseudonymised" under the GDPR[25] when it is processed in such a way that it can no longer be linked to a specific individual without using any additional information. If the data is considered pseudonymised, it will remain subject to the requirements of the GDPR because of the possibility of re-identification by the controller who holds the key to re-identification.

On the other hand, data will be considered "anonymous" under the GDPR[26] when the information does not relate to an identified or identifiable individual or the data is anonymised so that the individual is no longer identifiable. Generally, whilst pseudonymisation may be reversed by the controller who holds the key, anonymisation should not be reversable. Like statistical data, anonymous data will not be subject to the GDPR because it does not constitute personal data.

The GDPR refers to the "means reasonably likely" test which essentially means that the party should consider what means, such as other information, technology or research methods, are available and reasonably likely to be used by the party or "another person" to identify the individual. Account should be taken of "all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".[27] So whilst anonymisation should generally not be reversable in order to be effective, the GDPR acknowledges that absolute anonymisation may sometimes be difficult and anonymisation will be effective even if the data is hypothetically reversable but not without significant effort, i.e. effort that would be too expensive, too time consuming, or too demanding on technology. Indeed, if personal data is not sufficiently stripped of elements and it remains possible by using "reasonably available means"[28] to re-identify the individual, that data will merely be pseudonymised and not anonymised.

To deal with the different motivations and access to resources that the party or "another person" may have, the ICO refers to the "motivated intruder"[29] test. The motivated intruder is a presumed character who has no prior knowledge but who wishes to identify the individual. They are reasonably competent, have access to resources such as public information and would employ common investigative techniques to achieve his or her goal.

In the Breyer case,[30] the CJEU held that data will not be personal *"if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant"*. The court took a subjective approach by looking at the party that holds the data and considering if that party may have access to any third party data that would reasonably likely be used by that party to combine such third party data with its own data to identify an individual.

Similarly, the ICO's Anonymisation code of practice ("ACP"),[31] referencing the case of *R (Department of Health) v Information Commissioner*,[32] confirms that if an organisation converts personal data into an anonymised form and then subsequently shares it with another organisation, this will not amount to a disclosure of personal data to that receiving organisation, despite the disclosing organisation still holding the key to re-identification.

Finally, data will generally not be anonymous if it allows for an individual to be "singled out", i.e. identified on the basis of information such as an IP address or a unique identifier, even if their actual name is not known.[33] This concept has been used in connection with online behavioural advertising that uses profiles about individuals only distinguished through a unique identifier to deliver ads to their machines without knowing their actual identity. However, the ICO does not seem to take such a broad view in relation to anonymisation. In its ACP (not updated since 2012) the ICO suggests that data will not be personal data in the hands of a party which is not in possession of nor is likely to hold a key which would allow for re-identification, even if each individual is distinguished through a unique identifier.[34] The ICO took that view despite the "singling out" concept which dates back to at least 2007. Whilst there is a risk that this interpretation may change in future as effective anonymisation becomes more difficult with the rise of technological capabilities, we believe that the code remains good advice.

3 Privacy in wellbeing

(a) Privacy and wellbeing devices

Health in the context of privacy has been a broad concept since the Court of Justice of the European Union's decision in Lindqvist[35] where the Court held that data concerning health must be given a wide interpretation and should include all aspects of the physical and mental health of an individual. The scope of this concept was further clarified by the WP29 in its response to the European Commission. The WP29 particularly considered this concept in relation to lifestyle and wellbeing apps[36] and

© Published and reproduced with kind permission by Global Legal Group Ltd, London

set out particular criteria to determine when data processed by apps and devices constitute health data. The notion of health data as a broad concept was translated into the definition of "data concerning health", which is separately defined under the GDPR and the scope further clarified in Recital 35 of the Regulation.

The WP29 considered that devices which tested an individual's urine and blood, or apps measuring blood pressure or heart rate, would be considered as "information derived from the testing or examination of a body part of bodily substance, including biological samples", and would therefore fall under the definition of health data under the GDPR. The WP29 emphasised that whether the testing is performed by medical professionals or whether the devices are marketed as strictly medical devices are not relevant factors to consider in this context.

Similarly, data relating to the potential future health of an individual would be considered as information about "disease risk" which would also fall under the definition of health data under the GDPR. This type of data could include information about an individual's weight, blood pressure, hereditary or genetic conditions, alcohol/tobacco/drug use or any other information that has the potential to imply a risk of disease in the future. Wellbeing devices which are able to identify disease risk by analysing exercise or dietary habits to determine whether particular lifestyle habits could impact the risk of the disease would be considered as collecting health data, whether the actual raw data collected from the individual was not in fact their health data. However, the WP29 limits the scope by stating that not all raw data collected from apps can be considered as data concerning the health of an individual. The example provided is an app which counts the number of steps during a walk without combining this data with any other information about the individual. The justification for this distinction is because this type of data does not warrant the additional layer of protection afforded to special category personal data, including health data.

On the other hand, the WP29 reiterated the importance of exercising caution in relation to personal data which, if used for a particular purpose or combined with other information about the individual, may be considered health data. For example, an individual's weight or heart rate alone may not indicate the health status of an individual, however, if this data is recorded over a period of time and combined with the individual's age or gender, it may reveal health risks related to obesity or blood pressure. These revelations should always be considered health data. In the context of lifestyle apps, this means that an app simply recording the calories inputted by the individual user would not be considered to collect health data. However, if data from this app was linked with the individual user's social media profiles and an inference was drawn about that individual's health, this combined data would be considered health data.

As with the collection of other types of special category personal data, the most appropriate legal basis for the collection of health data by wellbeing devices and lifestyle apps is the individual's explicit consent.

(b) Purpose limitation, data minimisation and security

Organisations processing health data must comply with the key data protection principles of the purpose limitation and data minimisation when processing personal data. This means that personal data should only be collected for explicit, specific and legitimate purposes and should only be adequate, relevant and limited to what is necessary. In the context of special category personal data, including health data, this is even more important as the misuse of this type of data can have more detrimental consequences for the individuals affected in comparison to non-sensitive personal data. The WP29 clarifies that where further processing of health data is required for different purposes, these purposes are limited, and the burden is on the organisation processing the data to determine compatible and legitimate purposes.

Importantly, organisations processing health data must also have technical and organisational measures in place to ensure the principle of data minimisation is effective. These should include that only the absolute minimum amount or type of personal data required for a purpose is processed. Personal data should be pseudonymised where this is compatible with the research purpose, and personal data should not be used where the research purpose can be achieved by using anonymised data instead.

Moreover, organisations holding health data may be more vulnerable to personal data breaches and security incidents due to the inherent value in detailed information about individuals' health and the potential for hackers to monetise this information. IBM's report[37] highlighted that data breaches in the healthcare industry are the most expensive, costing an average of $6.45 million on average in 2019. It is clear that organisations processing health data need to implement more sophisticated security mechanisms to "ensure a level of security appropriate to the risk"[38] of processing health data.

(c) Data sharing and monetisation

The ICO, in its draft Data Sharing Code of Practice,[39] makes clear that in order to share special category personal data, including health data, organisations must have both a lawful basis and a special condition for doing so. Fairness and transparency are key principles in any data sharing arrangement and organisations responsible for sharing any personal data must ensure that the sharing is reasonable and proportionate. Individuals must be informed if their data is being shared, which organisations are sharing their data and which ones have access to their data.

In the world of healthcare, the sharing of data, particularly in a truly anonymised form, is crucial to developing the health data economy and producing clinical advancements which would not be achievable otherwise. However, there are concerns within the industry about individuals' health data being shared with large technology companies without knowledge or consent from these individuals. An investigation[40] into the top 100 health websites revealed that the majority of these websites had been unlawfully sharing website users' health data with participants within the AdTech industry. In fact, 79% had reportedly activated third-party advertising cookies on their websites without asking for consent from website users. This was a clear violation of both the GDPR and legislation governing the use of cookies (the Privacy and Electronic Communications Regulations 2003 ("**PECR**"). The health websites failed to both (a) gain explicit consent, as required under the GDPR, from website users for the sharing of their health data with advertisers, and (b) consent from website users for the use of targeted advertising cookies.

Arguably this unlawful sharing of data has potential negative consequences for individuals, particularly when the sharing of this data results in conclusions being drawn about individuals' health status. For example, this investigation uncovered that leading health websites were sharing information about individuals' symptoms, diagnoses, menstrual and disease information with leading advertisers and ad brokers. This information could then be linked back to the individual website user via a specific identifier linked to the web browser. The WP29[41] highlighted this potential harm by arguing that this health data could be used to draw conclusions about individuals' health in potentially "negative and/or unexpected ways" which could have unjustified adverse effects on the individuals.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Endnotes

1. There are four classes of general medical devices, as follows: Class I – generally regarded as low risk; Class IIa – generally regarded as medium risk; Class IIb – generally regarded as medium risk; and Class III – generally regarded as high risk.
2. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices.
3. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices.
4. Article 35(1) GDPR says that you must do a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of individuals: "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*"
5. Article 28 GDP.
6. Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials and medicinal products for human use.
7. Article 13 GDPR.
8. https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf.
9. Article 9(2)(i).
10. A Preliminary Opinion on data protection and scientific research, dated 6 January 2020.
11. Opinion 3/2019 concerning the Questions and Answers on the interplay between the CTR and the GDPR.
12. Article 6(1)(C) GDPR.
13. Article 9(2)(i) GDPR.
14. Article 6(1)(a) GDPR and Article 9(2)(a) GDPR.
15. Article 9(2)(a) GDPR.
16. Article 6(1)(e) or (f) GDPR with Article 9(2)(i) or (j) GDPR.
17. A Preliminary Opinion on data protection and scientific research, dated 6 January 2020.
18. https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance.
19. Article 17(2)(b) GDPR.
20. A Preliminary Opinion on data protection and scientific research, dated 6 January 2020.
21. Article 17(2)(d) GDPR.
22. A Preliminary Opinion on data protection and scientific research, dated 6 January 2020.
23. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/.
24. Recital 57 GDPR.
25. Article 4(5) GDPR.
26. Recital 26 GDPR.
27. Recital 26 GDPR.
28. "What is personal data" section on the ICO website.
29. Anonymisation: managing data protection risk code of practice, ICO, November 2012, https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.
30. *Patrick Breyer v Bundesrepublik Deutschland* C-582/14.
31. Anonymisation: managing data protection risk code of practice, ICO, November 2012, https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.
32. *R (on the application of the Department of Health) v Information Commissioner* [2011] EWHC 1430 (Admin).
33. Page 13, Opinion 4/2007 on the concept of personal data, Article 29 Working Party, 20 June 2007; Para 3.2.2, Opinion 2/2010 on online behavioural advertising, Article 29 Working Party, 22 June 2010, and Recital 26 of the GDPR.
34. Page 59, Anonymisation: managing data protection risk code of practice, ICO, November 2012.
35. *ECJ Case C-101/01.*
36. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf.
37. https://www.ibm.com/security/data-breach.
38. Article 32(1) GDPR.
39. https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf.
40. https://www.ft.com/content/0fbf4d8e-022b-11ea-be59-e49b2a136b8d.
41. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Marta Dunphy-Moriel is a Partner in Kemp Little's Data Protection & Privacy practice and has worked closely with a range of businesses to achieve compliance using her experience working on privacy aspects of commercial contracts and procurement. She has deep knowledge of the impact of privacy in the health sector, including experience in dealing with privacy issues in clinical trials and digital health and wellbeing devices. She has assisted numerous UK-based and international organisations with the roll out of data protection/GDPR compliance projects, advised on privacy and AI (with a special focus on Digital Health), data sharing, data export solutions and BCR, cookies and similar technologies, privacy impact assessments, privacy by design, user rights, SARs, disclosure to authorities and data breaches.

Kemp Little
138 Cheapside
London, EC2V 6BJ
United Kingdom

Tel: +44 207 710 1618
Email: marta.dunphy-moriel@kemplittle.com
URL: www.kemplittle.com

Hayley Davis is a Managing Associate in Kemp Little's Commercial Technology practice and co-leads the Digital Health practice. She has a broad range of experience within the Digital Health sector, predominantly drafting and negotiating technology and general commercial agreements, assisting clients on all levels of the supply chain and assisting throughout the process from initial conception to final roll-out. Hayley also regularly advises on medical regulatory as well as data protection and privacy issues.

Kemp Little
138 Cheapside
London, EC2V 6BJ
United Kingdom

Tel: +44 207 710 8019
Email: hayley.davis@kemplittle.com
URL: www.kemplittle.com

Glafkos Tombolis is a Partner in Kemp Little's corporate practice and co-leads the Digital Health practice. Glafkos advises a broad range of corporate, institutional and private clients on private and public M&A transactions, private equity investments and general company law matters. He has particular expertise in the Digital Health sector, supporting a number of large corporates on strategic M&A transactions. Glafkos joined the corporate group in 2012 from Charles Russell Speechlys where he advised on both corporate matters and commercial arrangements for corporate, institutional and private clients. Glafkos started his career at Freshfields Bruckhaus Deringer, where he spent five years in the London corporate department upon qualification there.

Kemp Little
138 Cheapside
London, EC2V 6BJ
United Kingdom

Tel: +44 207 710 1672
Email: glafkos.tombolis@kemplittle.com
URL: www.kemplittle.com

Aneka Chapaneri assists clients across varied industry sectors with their general data protection compliance including drafting, negotiating and advising on data protection clauses in various types of agreements; advising in relation to direct marketing and online behavioural advertising issues and advising on and managing data breaches and data subject access rights requests. In the healthcare sector, Aneka has advised health-tech companies on data protection issues raised in corporate deals (due diligence, warranties and data processing agreements) and has conducted data protection impact assessments for high-risk processing activities.

Kemp Little
138 Cheapside
London, EC2V 6BJ
United Kingdom

Tel: +44 207 710 1631
Email: aneka.chapaneri@kemplittle.com
URL: www.kemplittle.com

Kemp Little is one of the UK's leading technology law firms; we began as purely IT lawyers and technology has remained our core focus ever since. Because technology is at the heart of everything we do, our lawyers are exposed to the nuances of technology-driven business on a daily basis.

As a specialist technology legal services firm, we act for sector-leading organisations across a range of technology, digital media and communications industries and in sectors where technology is fundamental to an organisation's operations and success. Our focus on providing practical business solutions to our clients means that we increasingly involve non-legal business consultants and specialist technology, some of which we have built in-house, to deliver results.

Our clients range from global technology and digitally focussed businesses (including over 20 in the *FTSE 100/250* and *Global Fortune 500*) to fast-growth venture backed companies and owner-managed businesses. Whilst each client has specific needs and goals, they come to us for the same thing: unrivalled sector knowledge and legal excellence.

www.kemplittle.com

KEMP LITTLE

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Issues in Equity, Cost-Effectiveness and Utilisation Relating to Digital Health


Jen Maki, Ph.D.


Susan H. Manning, Ph.D.


John Maruyama

The Center for Healthcare Economics and Policy, FTI Consulting

Introduction

Digital health refers to the intersection of information and communications technology (ICT) with healthcare.[1] By leveraging the technological advancements of the Digital Revolution, digital health has the potential to increase access to high quality care and reduce inefficiencies associated with healthcare delivery. Digital health broadly includes mobile health (mHealth), telehealth and telemedicine, but its scope is constantly evolving in response to new technology (particularly in the realm of data collection, storage and analysis[2]). Recent digital health offerings comprise of an array of products and services that include online medical booking,[3] genetics tests,[4] and even gamified mobile apps designed to incentivise healthy activity.[5] Each of these technologies has the benefit of being oriented toward individual consumers, responding to their needs and offering the potential of personalising outcomes. Ultimately, these technologies will bring disruptive changes to the healthcare framework that will fundamentally alter the roles of patients, providers, payers, industry, and regulators.

Digital health has experienced strong investment trends with the potential for immense financial gains in the coming future. Its financial growth has been just as remarkable as the technological advancements that drive it, with a current value at $86.4 billion and expectations of further astronomical growth: some firms estimate compound annual growth rates (CAGR) over 27% over the next decade and a market value of more than $500 billion by 2025.[6, 7] This growth is driven by both established firms and startups with the latter raising more than $8.1 billion in funding in 2018 alone and more than half of all deals were made for seed and series A rounds.[8] If these trends continue, digital health will have more than quintupled in size by 2025, with even more diverse offerings for consumers and providers.

While there has been tremendous technological and financial growth in this space, attention is often centred on the promise of these technologies with relatively little concern focused on potential inherent risks. These risks include issues relating to equity, effectiveness, value, and use. Digital health can expand access to care and, through AI and Machine Learning, may lead to more effective and efficient care delivery. However, these gains may not be distributed evenly across the population. Without well-informed and meaningful intent, digital health apps and related services may alienate some segments of the population. Machine Learning that is informed by data and samples not representative of the population may decrease quality of care and outcomes from those underrepresented in the data. Those that are underrepresented are often the most vulnerable, further compounding the issue.

The rapid proliferation of digital health has occurred in an environment with few checks and balances. There currently exists no reliable regulatory framework for evaluating the effectiveness or validity of digital health applications, and the lack of formal standards could prove detrimental to the digital health market due to the proliferation of ineffective technologies.[9] This can already be seen in the mobile health market, where a study of 280 diabetes monitoring applications found that only five applications had adequate health outcomes supporting the effectiveness of the product.[10] The study also noted that current literature on mHealth effectiveness is methodologically inconsistent and that it is difficult to design reliable control groups that distinguish the internal and external effects of app use. Since the burden of establishing effectiveness falls on consumers, this exacerbates the difficulties in gauging effectiveness due to the inherent variability of preferences and technological literacy.[11]

To overcome these difficulties, groups such as the NHS have established initiatives to create, apply, and evaluate metrics, as well as to establish resources such as a Digital Apps Library – a resource that contains a register of apps that have proven to be reliable, usable, and safe.[12] Such efforts will be instrumental to improving transparency and grounding technology on the needs of consumers. However, cost evaluation will remain difficult in the foreseeable future and will require a more comprehensive approach to evaluate outcomes.

The use and adoption of digital health is likely to completely transform care delivery as we know it today. While uptake by patients and healthcare providers can benefit that segment of the population, concerns such as supply-induced demand and spillover effects exist. Increasing access to care and lowering the cost has the potential to encourage use and may lead to higher levels of low value healthcare utilisation. Uptake of offerings such as Telehealth by some providers may shift the patient mix served by providers in a particular region and may lead to cream-skimming whereby providers attract lower cost patients and increase the profitability of their practice, while other competing practices suffer.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Digital health will undoubtedly play a critical role in healthcare moving forward. The enormous financial and technological growth underpinning digital health is indicative of a vibrant industry that will continue to grow over the coming decade. The development of effective regulations and quality measures will require full engagement from consumers, providers, and developers to ensure that technology is properly regulated, and researchers will need to develop a framework for evaluation with a consensus on methodology. Despite these concerns, digital health promises a future focused on the consumer, and along with that, the possibility of an evolutionary leap in healthcare.

Equity

Striking inequalities exist within healthcare and these inequalities can profoundly influence wellness, health outcomes, and longevity. In the United States, there exist differences in healthcare utilisation, access, and insurance coverage by race and socio-economic status. Although efforts through the Affordable Care Act in the US and NHS/PHE in the UK have narrowed the gap, significant disparities remain. One striking example is found in maternal mortality. In the US, the pregnancy-related death rate for black women is over three times higher than that of white women. This difference is driven in large part by community factors (e.g. housing), factors related to receipt of care in a facility, and patient risk factors.[13] Disease prevalence also varies among racial, geographic, and socioeconomic groups. Diabetes prevalence among black adults during 2013-2015 was estimated to be just over 12% compared to a prevalence of 7.4% for non-Hispanic whites and 8 percent for Asians.[14]

Many of these inequalities can be traced to social determinants of health, a set of factors that encompass the environment in which people live, work and age. Specifically, social determinants of health (SDOH) include: socioeconomic status, neighbourhood and built environment, health and healthcare, food, social and community context, and education.[15]

While health outcomes are driven in part by certain immutable factors such as genetics, the realisation that much of health and wellbeing is influenced by SDOH has spurred action toward addressing these factors. In this context, digital health holds much promise, particularly related to education and healthcare access. However, the proliferation of digital health should not be viewed as a panacea as many disparities are rooted in long standing, deeply rooted inequities. Without due care, digital health technologies may even further increase existing inequities.

In earlier years, differences in access to the Internet and technology presented an obstacle to the access and use of digital health resources. Individuals without financial means to own a cell phone or obtain internet access were necessarily precluded from utilising these resources. However, with current cell phone ownership estimated to be at or above 94% in the US and 93% in advanced economies, this is becoming much less of a concern.[16] Focus is now centered more on differences across the population in their use of such technologies and how these differences impact outcomes.[17]

Digital health technologies are often offered under a "one-size fits all approach". This is problematic and will limit the potential associated with these technologies. At the extreme, it may even cause harm. How a user interacts with a platform and how they respond to messaging is influenced by his or her own demographic and socioeconomic characteristics. In light of this, care must be taken to account for an individual's background, and messaging and material design should be culturally appropriate. An individual's level of education will also impact how they use digital health technology.

Education can have a profound influence on health. It is well-known that individuals with greater educational attainment experience higher levels of health and wellbeing than their less educated peers. This difference, in turn, further contributes to health disparities. While some of the impact of education is related to the ability to process complex information and perform strategic decision making, it also influences an individual's health literacy. Health literacy is defined as "the degree to which individuals have the capacity to obtain, process, and understand basic health information and services needed to make appropriate health decisions".[18] Health literacy is correlated with both health outcomes and health system costs, with low literacy leading to reduced health outcomes and higher costs.[19]

eHealth literacy is similar to health literacy and is defined as "the ability to seek, find, understand, and appraise health information from electronic sources and apply the knowledge gained to addressing or solving a health problem".[20] Research shows that an individual's level of health literacy is not highly correlated with access to, or the use of, digital health technology. However, it does influence the means by which individuals likely interact with and access information and will shape overall individual experiences.[21] A recent study found that individuals with low literacy levels were more likely to report that finding information from websites was difficult and frustrating as compared to those with higher levels of literacy. They are also less likely to search for information.[22] This is consistent with findings from other research which shows that information presented on health-related websites can be overly complex.[23] Text messaging, on the other hand, is a preferred means of communication for individuals with low levels of literacy. Taking these considerations into account, providers of digital health technologies can create interfaces and communication channels that promote equity *and* engagement.

One of the most promising areas of digital health and the impact it can have on equity is through improving access to care. Approximately one fifth of the US population resides in rural areas with inadequate access to care.[24] Digital health technologies, including telehealth and telemedicine, hold enormous potential to expand access to high quality care to those that are chronically underserved. Collectively, they capture education, patient engagement, utilisation management, preventative care, patient mobile health (i.e. wearables and apps), billable clinician to clinician/patient interaction, and clinical remote monitoring.

Remote interactive clinical services have tremendous potential in improved healthcare access. This can include both patient-to-provider interaction or provider-to-provider connections where a specialist can advise a generalist or other healthcare professional, such as a nurse practitioner, in real time. Residents in rural communities that would previously have had to travel long distances and incur additional costs related to travel to see a specialist may be able to receive care remotely via telehealth. Even routine care can be provided to patients living in medically underserved areas. For example, a rural health centre can have a nurse onsite directly interacting with the patient while a remote doctor performs the exam using video technology.

While the use of telehealth has grown dramatically over the last several years with changes in both regulations relating to reimbursement of services, and availability of these services fueling strong growth, it still represents a small fraction of physician-to-patient encounters. Physicians are exhibiting greater use of telehealth: physician use of telehealth has increased 340% in three years, growing from a utilisation rate of 5% among physicians in 2015 to 22% in 2018.[25] According to analysis of 29 billion private healthcare claims between 2014–2018, the growth varies dramatically by category.[26] Between 2014 and

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2018, telehealth use between a provider and a patient unrelated to a hospitalisation increased over 1,000%. Both the level of overall utilisation and growth are highest in provider-to-patient telehealth occurring outside a hospital setting. Discharge-related telehealth showed the second highest growth rate, and provider-to-provider had the lowest rate of growth.

While the potential for enhanced access exists, it may not be realised if certain segments of the population are less likely to utilise this technology. A recent J.D. Power survey found that only 9.6% of Americans reported ever having used telehealth services.[27] A staggering number – 74.3% of those surveyed – indicated that they were unaware or unable to access telehealth. Awareness was particularly low in rural areas, which are generally medically underserved regions that can benefit greatly from improved healthcare access made possible through telehealth.

Use of these services also varies by patient age. Those reporting that they had used telehealth were more likely to be young. Individuals in the 18–24 age group report the highest use (13.1%), but adults in the 35–44 age group report the second highest use (11.8%). Seniors report the lowest use (5.3%). Geographic location also matters. Use is highest among patients located in the western region of the US (11.1%) and lowest in the northeast region (5.7%). Individuals also differ in their views regarding the cost of telehealth. One half of Americans believe that provider visits utilising telehealth costs less than a traditional doctor's visit, but the other half believe it costs the same or more. As cost is a constraint that leads to individuals foregoing or delaying medical care, inaccurate assumptions regarding the cost related to telehealth may impede uptake. While differences in beliefs about the value of telehealth exist, the potential to expand access to care will be constrained.

Using artificial intelligence (AI) to provide both higher quality and more efficient care is a burgeoning area in the digital health space. Machine learning can be used to process tremendous amounts of data to identify patterns and produce insight that will impact the way healthcare providers deliver care. AI is being used to optimise administrative workflows, aid in diagnostics, wellness, and to improve operational technologies.

AI-assisted robotic surgery can produce superior outcomes by reducing complications. In this context, a patient's pre-op medical records are analysed to guide the surgeon's instrument. A study by Harvard Business Review found that AI-assisted robotic surgery has the potential to significantly reduce patient post-operative length of stay and could save billions annually in healthcare costs.[28]

AI can also be used to improve efficiency in imaging analysis. One study investigating the time it took to identify specific lung nodules found that automated analysis resulted in more efficient identification. AI could match and identify a nodule as much as 97% faster than that achieved by radiologists. At the very least, this has important implications for radiology workflow and could significantly reduce the time to diagnosis – adding both physician and patient value.

Another promising area falls in the clinical judgment and diagnosis space. Diagnoses can vary from one medical provider to another, and this is especially true when it comes to rare diseases. But because AI can consume and process tremendous amounts of information, it may be used to identify diseases more quickly – and more accurately – than using more conventional means.

While this area holds much promise, the very reliance on data to inform machine learning presents tremendous equity concerns. It is well-noted that clinical trials have far too little racial and ethnic diversity among their study population.[29] If data that informs AI is based on homogenous samples, that may lead to bias in the understanding of factors that impact a disease state or medical outcome. In the most harmful sense, it could lead to sub-optimal care for racial and ethnic minorities.

Recent research highlights this concern. Health systems and payers routinely use technology to identify patients for "high-risk case management". These are patients with complex care needs that will benefit from care coordination and greater resources. To identify the correct target population, health systems and payers rely on commercial risk-prediction tools. These tools are based on proprietary algorithms to create a risk score for each patient. Since the algorithm is proprietary, the process lacks transparency, reducing the user's ability to "look under the hood" and ensure the process is fair and equitable.

In an effort to test for bias in these scores, a team of researchers worked with a large academic medical centre to review patients enrolled in risk-based contracts from 2013–2015.[30] They reviewed medical records and patient information, as well as the risk score generated for each patient. Their findings showed that the algorithm was indeed biased. While a black and a white patient might have received the same risk score, the black patient was sicker, on average. This means that risk scores for black patients were skewed downward. The effect of this bias reduced the percentage of black patients enrolled in the programme under study and effectively reduced the probability that that same patient would receive extra care that should have been offered.

Cost-Effectiveness

One of the key benefits of telehealth is that it can theoretically reduce travel and patient costs while increasing access to care. These factors are important when considering treatment for chronic (long term) conditions, such as diabetes or chronic obstructive pulmonary disease – conditions with high prevalence rates in both the United States and United Kingdom. Recent studies have shown that approximately 60% of American adults suffer from at least one chronic condition and collectively cost $1.1 trillion in healthcare costs, not including losses in productivity.[31] In the UK, 15 million Britons have at least one chronic condition and account for as much as two-thirds of all NHS spending.[32] These grim statistics motivate the potential that technology and policy can play in keeping care affordable and accessible.

While the use of telehealth can hold promise in treating patients with chronic conditions, it is not a "silver bullet", singularly able to moderate high healthcare spending. Some telehealth services may have a strong positive impact on the patient's health and wellness, while others may be less effective. As patients and payers look to sort through the massive amounts of offerings to identify those services that provide true value, information on cost-effectiveness and willingness to pay becomes crucial. Cost-effectiveness analysis is used to examine the costs and health outcomes of an intervention by comparing it against another intervention (or the *status quo*) to estimate the costs it takes to gain a unit of some positive outcome.[33] An example of cost-effectiveness analysis would be to compare the cost required to generate one unit of health from a school lunch program (relative to the *status quo*), where lower net costs indicate greater savings. Both cost-effectiveness and willingness-to-pay analyses can be used to empirically evaluate the effects of telehealth programs and to develop objective benchmarks to gauge worthwhile programs and services.

Studies have used these types of analyses to demonstrate that outcomes can be substantially different from the use of digital health as a care substitute versus a supplement, where the latter can result in enormous costs compared with small benefits. It must be noted that most of these studies are on telehealth,

© Published and reproduced with kind permission by Global Legal Group Ltd, London

with few existing for other digital health technologies. Even for telemedicine evaluations, there are limitations in evaluating economic impact due to a lack of randomised control trials, small sample sizes, and the absence of quality data and appropriate measures. Nevertheless, numerous studies have been conducted to evaluate the quality and cost-effectiveness of telehealth – some of which have gone as far as developing metrics against which to gauge effectiveness.

An important cost-effectiveness study conducted by Henderson, *et al.* (2013), compared the cost and cost-effectiveness of telehealth services with those of standard support and treatment alone in the United Kingdom.[34] Using funding and sites provided by the United Kingdom's Whole Systems Demonstrator (WSD) program, the authors examined the effect of telehealth on primary, secondary, and social care for individuals with chronic obstructive pulmonary disease (COPD), heart failure, or diabetes. The sample was randomised between usual care or a telehealth intervention in addition to standard care in a trial that recruited 3,230 participants between May 2008 and December 2009. 1,573 patients completed a questionnaire used to evaluate outcomes, effectiveness and patient perspective on the telehealth supplement. Of these participants, 728 were randomised to usual care and 845 to the telehealth intervention: 965 patients had both outcomes and cost data at both the baseline and a 12-month follow-up.

The telehealth interventions included both monitoring equipment that collected and transmitted data to create risk-related alerts and the ability for patients to communicate with health professionals who could provide health education information. The outcome measure was incremental cost per quality adjusted life year (QALY). While the costs of the telehealth group were lower than those of the usual excluding intervention costs (12% difference between groups), they were higher when intervention costs were included (10% difference between groups). At the £30,000 WTP threshold recommended by the National Institute for Care and Excellence (NICE), the program was not cost-effective. Most importantly, even with assumed reductions, the probability of cost-effectiveness was only 61% at the £30,000 level, which indicates that telehealth, in this particular scenario, was not cost-effective as a supplement to standard care.

A study from Eckman (2018) compared the cost of a primary care focused digital model with a traditional care model in Sweden.[35] The author used the 2015 national mean of costs per care contact in primary care to measure the direct and indirect costs of both models. The author assumed that the direct costs for a traditional model would include staff renumeration, lab costs and diagnostic services; the indirect costs were assumed to include administration and support, management, office and equipment rents, and investment write-offs. The direct and indirect digital costs for the digital plan were obtained from a Swedish digital care provider company. Captured patient costs included user fees, time, and travel costs. The findings showed that traditional care is less expensive for patients, costing the equivalent of $21 USD *versus* $29 USD. However, digital treatment took less time than traditional care at 15 minutes per patient on average, versus 24 minutes for traditional treatment. The results of this analysis were used to determine cost-effectiveness, simulating substitution rates ranging between 10% and 50%. Total societal costs were lower for digital care at $222 USD per unit cost compared to $380 USD for traditional care: a difference of 40%. This can be attributed to the lower user costs for digital care, which creates a 51% cost difference due to time costs for the consultation. At a 10% rate of substitution, $229 million USD would be saved annually; savings jump to $565 million USD at a 50% rate of substitution. This study suggests that telehealth can be quite cost-effective as a substitute for traditional care in this context, when considering the monetary costs associated with healthcare.

It is important to note that the prior study suggests not only significant monetary savings, but time savings as well. While these two factors often go together, they are not mutually exclusive, and other studies suggest that telehealth can provide time savings, even in the absence of cost savings. A study from Egede, *et al.* (2017), compared telehealth treatment with in-room treatment for older veterans.[36] The results demonstrate that there is no difference in cost of care and both modalities were found to provide effective care. While the article does not discuss time and travel costs, these would likely result in savings if brought into consideration. A study by Pyne, *et al.* (2015), found that participants receiving care via telemedicine had more depression free days, but treatment costs were higher overall.[37] The increase in cost could be attributed to the increase in volume/utilisation.

As telemedicine interventions in the mental health sphere are commonly used to combat the dearth of mental health resources, this modality of care can represent an effective, and cost-effective, means to provide treatment. This is especially so when patient costs (transportation costs) are taken into account.

The rural health sector is a sphere where telehealth can provide the most compelling net benefits. Due to long travel times and physician scarcity, particularly relating to specialists, residents in rural communities often struggle to receive the care they need. A study by Kessler, *et al.* (2016), examined whether telehealth would be effective in countering problems relating to the travel time patients often face when seeing pediatric rheumatologists; rural patients often undertake long-distance travel due to the scarcity of doctors in this specialty.[38] The authors found that telemedicine can reduce the time burden associated with care, especially missed school days. An article by Yang, *et al.* (2015), studied the provision of video and telephone consultations to children in rural emergency departments (EDs) and how these two separate modalities of care related to total treatment cost and probability of being transferred to another location.[39] Results showed that children receiving a video consultation were less likely to be transferred to another ED and were less costly than those receiving a telephone consultation. These studies suggest that there are notable cost and social benefits to introducing telehealth initiatives to rural communities.

Telehealth benefits can also be realised in older adults. In a study by Upatising, *et al.* (2015), the authors examined the cost-effectiveness of supplemental telemedicine care for older adults.[40] The results showed that participants receiving telehealth care had lower variability of care and lower 30-day readmission costs, but there were no significant differences in total cost of care compared with the control group. However, when considering the social benefits and impact on wellbeing associated with achieving lower readmission rates, telehealth, in this context, may still be beneficial.

The foregoing studies demonstrate that when considering cost-effectiveness, it is important to weigh the full set of costs and benefits – including factors such as productivity gains, wellness, and even other externalities that may result from the use of telehealth solutions.

Utilisation

Consumption of healthcare services is generally patient initiated. If an individual is ill or is seeking healthcare advice, he or she will contact a physician, initiating a healthcare-based relationship. This relationship and any associated receipt of healthcare services will generally continue until the patient's needs are met. Supply-induced demand is when the medical treatment

© Published and reproduced with kind permission by Global Legal Group Ltd, London

the patient receives exceeds his or her actual needs. The reason this may occur is because physicians are economic agents and, as with all economic agents, may be guided in part by their own financial interests. When physician compensation is impacted by the quantity of care they supply, this may lead to supply-induced demand. The net effect of this phenomena is to raise utilisation levels unnecessarily, such that they exceed what they would be if guided entirely by patient requirements.

The propensity for digital health to lead to supply-induced demand varies based on the funding scheme for healthcare services. Accordingly, supply-induced demand is more likely to occur when a physician is compensated for each service rendered than under capitation, where the provided receives a set amount to provide care for the patient, regardless of volume.

As mentioned already, digital health, and telehealth in particular, has the potential to increase access to care. Therefore, there is some expectation that healthcare utilisation will increase. What is challenging, however, is disaggregating changes in care utilisation stemming from suppressed demand from those relating to supply-induced demand.

To see this issue, consider an innovative primary care provider that offers patients the ability to interact digitally with healthcare providers and bypass the wait times generally required for traditional visits offered at traditional brick and mortar locations. While more immediate access to care is surely an attractive feature to registered patients, there are other important, related factors, to consider. For example, use of this "disruptive" technology may increase utilisation of care above optimal levels and have spill-over effects that impact traditional providers.

Transaction costs are part of the costs an individual incurs when receiving healthcare services. A prime example is the transportation time required to go from the patient's home or workplace to their doctor's office. Because this represents a real cost to the patient, he or she will weigh the value they place on seeing a healthcare provider with the cost they incur from the visit. If the benefit of the visit outweighs the cost, he or she will see their healthcare provider. If not, care will be deferred until such time when the benefit outweighs the cost.

When costs are low, as would be the case with telehealth where the patient can interact with the healthcare provider digitally using his or her smartphone, there is little incentive to defer care. While a patient experiencing a cough may have the incentive to wait a week or two to see if the issue resolves on its own, in the absence of transaction costs, that individual may opt to see a healthcare provider earlier on.

A review of utilisation of care from GP at Hand, an innovative digital healthcare provider in North West London, seems to suggest that easing access to care may result in increased utilisation. A recent article noted that GP at Hand's patients, individuals that have access to AI triage and video visits with healthcare providers, utilised more care than that of a similar demographic patient cohort.[41] However, the fact that utilisation is higher among GP at Hand's patients does not necessarily signal a change in health-seeking behaviour or supply-induced demand: it could benignly be the result of improving access to care and reducing possible pent up demand.

Where telehealth is used by only some providers, there may be negative spillover effects. The types of patients attracted to digital care may differ from the general patient population. The same article noted that 94% of GP at Hand's patients are under the age of 45 and two-thirds live in affluent geographic locations.[42] These patients may be healthier and have less complex health needs than the general population. And since the UK adopted the Patient Choice Scheme in 2015 which allows patients to register outside their traditional catchment areas, the "healthy" patients may self-select providers that offer digital care. In doing so, it can leave the patient mix in the traditional place-of-service GP practices leaning toward those with more complex care needs. Some of the potential impact of this concern is alleviated by the funding formula used to compensate the GP for patients that require a higher workload. However, skewing the patient mix toward those requiring more complex care could increase physician burnout and still reduce the GP's financial outcomes if the funding formula is not precise enough to capture differences in the workload associated with the characteristics of a particular patient population.

At present, it is difficult to disentangle the effects of suppressed demand from potential supply-induced demand. This is, however, sure to be an area of study. As use of telehealth services grow, this will provide a larger sample and a longer time frame over which to study the issue and inform the debate.

Conclusion

Digital health offers tremendous promise, with much potential to increase access to care, quality of care, and to transform the efficiency of care delivery. Telehealth can be used to improve health literacy which can lead to improved health outcomes and reduce some of the disparities that currently exist in healthcare delivery. Patients in geographically remote locations can benefit from using telehealth to connect with healthcare providers they would otherwise require lengthy travel to see. Even in urban areas where provider scarcity is not an issue, patients can benefit from reduced wait times and ease of access.

However, uptake and the full potential of telehealth will not be realised until stakeholders are able to address the important issues of equity, cost-effectiveness and use. Concerns about data used in machine learning may make users weary about the risk they face in relying on AI too heavily in the healthcare domain. The user interface and communication design may lead to disparities in use and limit the effectiveness of these technologies. Payers will be hesitant to cover services and associated technology if questions regarding the effectiveness go unanswered. If payers, providers, and regulators worry that digitised healthcare will be used to cherry-pick patients, use will be suppressed.

The solution to these problems is two-fold. The first speaks to the importance of awareness. As long as those that design and produce these technologies are aware of these issues, steps can be taken to ameliorate the harm that may result from the approach that assumes all people interact with data and messaging the same way. The second key is time and study. As more time goes by and data accumulates, leveraging real world data (such as claims data) will result in a much more comprehensive knowledge base than could ever be generated from case control studies. In fact, the use of real-world data is an increasingly important tool that providers of digital health technology rely on to promote their products and gain reimbursement. As this trend continues, it will be possible to create well-informed guidelines and resources to help users and stakeholders sort through the dizzying array of "solutions" in the space, to identify those that provide the most value.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Endnotes

1. There are many definitions of digital health: this definition reflects the general scope of the digital health sector.
2. Dash, S., Shakyawar, S.K., Sharma, M. *et al.* J Big Data (2019) 6: 54. https://doi.org/10.1186/s40537-019-0217.
3. https://www.zocdoc.com. (Accessed 12/19/2019.)
4. https://www.23andme.com. (Accessed 12/19/2019.)
5. Medical Futurist. *The Top 15 Examples of Gamification in Healthcare.* (Accessed 12/19/2019.) https://medicalfuturist.com/top-examples-of-gamification-in-healthcare.
6. Grand View Research. *Digital Health Market Size Worth $509.2 Billion By 2025 | CAGR 27.7%.* (Accessed 12/19/2019.)
7. Global Market Insights. Digital Health Market Size By Technology 2019-2025, Industry Trends. (Accessed 12/19/2019.)
8. Day, Zweig. 2018 Year End Funding Report: Is digital health in a bubble? (Accessed 12/12/2019.) https://rockhealth.com/reports/2018-year-end-funding-report-is-digital-health-in-a-bubble.
9. Mathews, S.C., McShea, M.J., Hanley, C.L. *et al.* Digital health: a path to validation. npj Digit. Med. 2, 38 (2019) doi:10.1038/s41746-019-0111-3.
10. Veazie S, Winchell K, Gilbert J, Paynter R, Ivlev I, Eden K, Nussbaum K, Weiskopf N, Guise J-M, Helfand M. Mobile Applications for Self-Management of Diabetes. Technical Brief No. 31. (Prepared by the Scientific Resource Center under Contract Nos. 290-2012-0004-C and 290-2017-00003-C.) AHRQ Publication no. 18-EHC010-EF. Rockville, MD: Agency for Healthcare Research and Quality; May 2018. Posted final reports are located on the Effective Healthcare Program search page. https://doi.org/10.23970/AHRQEPCTB31.
11. Mathews, S.C., McShea, M.J., Hanley, C.L. *et al.* Digital health: a path to validation. npj Digit. Med. 2, 38 (2019) doi:10.1038/s41746-019-0111-3.
12. https://www.nhs.uk/apps-library.
13. Petersen EE, Davis NL, Goodman D, *et al.* Vital Signs: Pregnancy-Related Deaths, United States, 2011–2015, and Strategies for Prevention, 13 States, 2013–2017. MMWR Morb Mortal Wkly Rep 2019;68:423–429. DOI: http://dx.doi.org/10.15585/mmwr.mm6818e1external icon.
14. Centers for Disease Control and Prevention. *Addressing Health Disparities in Diabetes.* 2017. https://www.cdc.gov/diabetes/disparities.html. (Accessed 1/21/2020.)
15. KFF. 2018. "Beyond Health Care: The Role of Social Determinants in Promoting Heath and Health Equity" https://www.kff.org/disparities-policy/issue-brief/beyond-health-care-the-role-of-social-determinants-in-promoting-health-and-health-equity. (Accessed 1/7/2020.)
16. Pew Research Center, 2019. "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally" https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally. (Accessed 1/7/2020.)
17. Manganello, Jennifer, Gena Gerstner, Kristen Pergolino, Yvonne Graham, Angela Falisi, and David Strogatz. "The relationship of health literacy with use of digital technology for health information: implications for public health practice." *Journal of public health management and practice* 23, no. 4 (2017): 380-387.
18. Institute of Medicine, 2004. *Health Literacy: A Prescription to End Confusion.* Washington, DC: The National Academies Press. https://doi.org/10.17226/10883.
19. Haun JN, Patel NR, French DD, Campbell RR, Bradham DD, Lapcevic WA. "Association between health literacy and medical care costs in an integrated healthcare system: a regional population based study." BMC Health Serv Res. 2015;15:249 and Howard DH, Gazmararian J, Parker RM. "The impact of low health literacy on the medical costs of Medicare managed care enrollees." Am J Med. 2005;118(4):371-377.
20. Norman CD, Skinner HA. "eHealth literacy: essential skills for consumer health in a networked world." J Med Internet Res. 2006;8(2):e9.
21. Manganello, Jennifer, Gena Gerstner, Kristen Pergolino, Yvonne Graham, Angela Falisi, and David Strogatz. "The relationship of health literacy with use of digital technology for health information: implications for public health practice." *Journal of public health management and practice* 23, no. 4 (2017): 380-387.
22. *Ibid.*
23. Eltorai AE, Han A, Truntzer J, Daniels AH. "Readability of patient education materials on the American Orthopaedic Society for Sports Medicine" website. Phys Sportsmed. 2014;42(4):125-130; Sharma N, Tridimas A, Fitzsimmons PR. A readability assessment of online stroke information. J Stroke Cerebrovasc Dis. 2014;23(6):1362-1367; and Walsh TM, Volsko TA. "Readability assessment of internet-based consumer health information." Respir Care. 2008;53(10):1310-1315.
24. Robin Warshaw. 2017. "Health Disparities Affect Millions in Rural U.S. Communities." AAMC. https://www.aamc.org/news-insights/health-disparities-affect-millions-rural-us-communities. (Accessed 1/7/2020.)
25. American Well, "Telehealth Index: 2019 Physician Survey" (2019) https://www.americanwell.com/resources/telehealthindex-2019-physician-survey.
26. FAIR Health, "A Multilayered Analysis of Telehealth." (2019).
27. J.D. Power. U.S. Telehealth Satisfaction Study. 2019 https://www.jdpower.com/business/press-releases/telehealth-usage-and-awareness-pulse-survey.
28. Kalis, Brian, Matt Collier, and Richard Fu. "10 promising AI applications in health care." *Harvard Business Review* 10 (2018).
29. Oh, Sam S., Joshua Galanter, Neeta Thakur, Maria Pino-Yanes, Nicolas E. Barcelo, Marquitta J. White, Danielle M. de Bruin *et al.* "Diversity in clinical and biomedical research: a promise yet to be fulfilled." *PLoS medicine* 12, no. 12 (2015): e1001918.
30. Obermeyer, Ziad, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. "Dissecting racial bias in an algorithm used to manage the health of populations. "*Science* 366, no. 6464 (2019): 447-453.
31. Buttorff, Christine, Teague Ruder, and Melissa Bauman, Multiple Chronic Conditions in the United States. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/tools/TL221.html, and Graf M, Waters H. The Costs of Chronic Disease in the U.S. Milken Institute Report. (Accessed 01/17/2020.) https://milkeninstitute.org/sites/default/files/reports-pdf/ChronicDiseases-HighRes-FINAL.pdf.
32. Long Term Conditions Compendium of Information. 3 Ed. (Accessed 01/17/2020.) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/216528/dh_134486.pdf and Full Fact. How much of the NHS budget is spent on

© Published and reproduced with kind permission by Global Legal Group Ltd, London

treating chronic conditions? (Accessed 01/17/2020). https://fullfact.org/news/how-much-nhs-budget-spent-treating-chronic-conditions.
33. CDC. Cost Effectiveness Analysis (CEA). (Accessed 01/16/2020.) https://www.cdc.gov/policy/polaris/economics/cost-effectiveness.html.
34. Henderson C, Knapp M, Fernandez J-L, Beecham J, Hirani SP, Cartwright M, Rixon L, Beynon M, Rogers A, Bower P, Doll H, Fitzpatrick R, Steventon A, Mardsley M, Hendy J, Newman SP. Cost effectiveness of telehealth for patients with long term conditions (Whole Systems Demonstrator telehealth questionnaire study): nested economic evaluation in a pragmatic, cluster randomised controlled trial. BMJ 2013;346:f2065. Doi: https://doi.org/10.1136/bmj.f2065.
35. Eckman B. Cost Analysis of a Digital Health Care Model in Sweden. PharmacoEconomics – Open. 2018; 347:354. Doi: 10.1007/s41669-017-0059-7.
36. Egede LE, Gebregziabher M, Payne EH, Acierno R, Frueh BC. Trajectory of cost overtime after psychotherapy for depression in older Veterans via telemedicine. Journal of Affective Disorders Online. 2017;157:162. Doi: 10.1016/j.jad.2016.09.044.
37. Pyne JM M.D., Fortney JC Ph.D., Mouden S M.S. C.R.C., Lu L M.S., Hudson TJ Pharm. D., Mittal D M.D. Cost-Effectiveness of On-Site Versus Off-Site Collaborative Care for Depression in Rural FQHCs. Psychiatric Services. 2015;491:499. Doi: 10.1176/appi.ps.201400186.
38. Kessler EA, Sherman AK, Becker ML. Decreasing patient cost and travel time through pediatric rheumatology telemedicine visits. Pediatric Rheumatology Online Journal. 2016;14:54. Doi: 10.1186/s12969-016-0116-2.
39. Yang N, Marcin J, Yoo B, Paul Leigh J, Romano P, Kuppermann N, Nesbitt T, Dharmar M. Economic Evaluation of Pediatric Telemedicine Consultations to Rural Emergency Departments. CMedical Decision Making. 2015; 73:783. Doi: 10.1177/0272989X15584916.
40. Upatising B, Wood DL, Kremers WK, Christ SL, Yuehwern Y, Hanoson GJ, Takahashi PY. Cost comparison between home telemonitoring and usual care of older adults: a randomized trial (tele-ERA). Telemedicine and e-Health. 2015;3:6. ISSN: 1530-5627.
41. Burki, Talha. "GP at hand: a digital revolution for health care provision?" *The Lancet* 394, no. 10197 (2019): 457-460.
42. *Ibid.*

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Jen Maki, Ph.D., is a Managing Director in the Center for Healthcare Economics and Policy at FTI Consulting. Her work includes the analysis and modelling of factors that drive demand for healthcare products and services and assessment of trends in the delivery of healthcare.
Dr. Maki regularly works with IMS data, commercial claims data and Medicare data to assess demand for healthcare products, price variation, and evaluate treatment patterns. She often works on litigation matters addressing liability and quantifying damages. Dr. Maki has also served as a testifying expert in litigation proceedings.
Dr. Maki is an active researcher and has written on topics including the effects of informational interventions on individual decision-making and on tobacco policies and their effect on smoking cessation. Her research articles have been published in peer-reviewed journals, including the Southern Economic Journal and the International Journal of Drug Policy.

FTI Consulting
Two North Central
Suite 1200
Phoenix AZ 85004
USA

Tel: +1 602 744 7157
Email: jen.maki@fticonsulting.com
URL: www.fticonsulting.com

Susan Manning is the Chief Operating Officer and Senior Managing Director of FTI's Center for Healthcare Economics and Policy. She has over 30 years of economics and litigation consulting experience, including extensive expertise in antitrust and competition issues, mergers and acquisitions, and regulatory policy analysis. She has provided economic analyses of healthcare related mergers and acquisitions before the US DOJ and US FTC, focusing on competitive effects and consumer welfare benefits of proposed transactions.
Dr. Manning has focused on assessing and modelling the impact of healthcare reform and structural change in meeting a population's present and future healthcare needs. This includes determining the most cost-efficient and best quality of care delivery structure for delivering healthcare within a community in light of the changing and broader mission of healthcare providers. Dr. Manning also has worked extensively in the UK on healthcare issues involving transformational change in the delivery of care.

FTI Consulting
555 12th Street NW
Suite 700
Washington DC 20004
USA

Tel: +1 202 589 3458
Email: susan.manning@fticonsulting.com
URL: www.fticonsulting.com

John Maruyama is a Consultant at FTI Consulting's Center for Healthcare Economics and Policy. He emphasises the use of data-driven methods through programs such as Python and Stata in conjunction with an innovative, holistic research strategy to inform policy decisions. Prior to joining FTI, he was a Research Assistant at Vanderbilt University where he examined the relationship between the history and policy of Medicare and Medicaid. Working under a grant from the NBER, he developed protocol for locating and synthesising hospital data that could be interpreted through STATA. He was also a Research Assistant at the University of Colorado Boulder where his focus was on the economic history of European capital and financial markets. His work included the documentation of data and development of methodology to filter and extract information from historical databases. His output is critical to an ongoing project that builds upon the existing literature in the field.

FTI Consulting
555 12th Street NW
Suite 700
Washington DC 20004
USA

Tel: +1 202 728 8726
Email: john.maruyama@fticonsulting.com
URL: www.fticonsulting.com

The FTI Consulting Economic Consulting practice provides law firms, corporations and government agencies with sophisticated and comprehensible analyses of complex economic issues to assist them in understanding the issues and opportunities they face. Our Economic Consulting practice is involved in a wide range of engagements related to economics, finance and accounting. We provide critical insight and expert testimony in legal and regulatory proceedings, strategic decision-making and public policy debates. We also have deep expertise in antitrust issues, mergers and acquisitions, securities litigation and risk management, valuation and international arbitration.
The Center for Healthcare Economics and Policy leverages cutting-edge methodologies, actionable metrics and economic analytics to facilitate organisational and community-based healthcare transformation strategies and initiatives. Our experts include Ph.D. economists and experienced healthcare professionals with extensive knowledge of healthcare economics, disease conditions, and state-of-the-art modeling. We help clients, including employers, providers, governments and community organisations, design and achieve implementable solutions grounded in robust data analysis to improve healthcare delivery.

www.fticonsulting.com

FTI CONSULTING
EXPERTS WITH IMPACT™

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Australia

Biopharmalex

Wayne Condon

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

The Australian Digital Health Agency states that the aim of digital health is to electronically connect different points of care so that health information can be shared securely. The technologies deployed to achieve this outcome are wide-ranging and include both hardware and software solutions and services including web-based analysis, medical software, mobile phone and tablet applications, email, wearable devices and telemedicine.

1.2 What are the key emerging technologies in this area?

The rate of technological development in personalised health and wellness is increasing exponentially. Some of the emerging technologies are personal genomics, machine learning and artificial intelligence (AI), smart medical devices, sensors and wearables and quantified self software.

1.3 What are the core legal issues in health care IT?

The core legal issues involve the regulatory overlay applicable to digital health, software as a medical device, confidentiality and cyber-security, and privacy.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The over-arching legislation by which therapeutic goods, including medical devices, are regulated in Australia is the Therapeutic Goods Act 1989.

2.2 What other regulatory schemes apply to digital health and health care IT?

Detailed and specific regulatory requirements are set out in the Therapeutic Goods Regulations 1990, the Therapeutic Goods (Medical Devices) Regulations 2002 and in various standards set out in therapeutic goods orders and codes. It is important to note that the regulation of digital health products will be dealt with under the existing framework for the regulation of therapeutic goods generally although there will be amendments dealing with specific issues and technologies, e.g. software as a medical device.

2.3 What regulatory schemes apply to consumer devices in particular?

In the area of digital health, medical device regulation provides the fundamental regulatory framework. Definitional elements become critical to the scope of regulation. Before a sponsor can import or supply a medical device in Australia, it must be listed or registered in the Australian Register of Therapeutic Goods (ARTG). A fundamental question, therefore, becomes whether a particular digital health development falls within the definition of a "medical device".

A *medical device* is:

"any instrument, apparatus, appliance, material or other article (whether used alone or in combination, and including the software necessary for its proper application) **intended**, by the person under whose name it is or is to be supplied, **to be used for** human beings for the purpose of one or more of the following:

1. diagnosis, prevention, monitoring, treatment or alleviation of disease;
2. diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability;
3. investigation, replacement or modification of the anatomy or of a physiological process; and/or
4. control of conception;

and that does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but that may be assisted in its function by such means" (emphasis added).

As can be seen from the definition of "medical device", it is the intended use of the device, which is critical, that has to be determined objectively.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The Therapeutic Goods Administration (TGA) is the regulatory body charged with administering and enforcing the provisions of the Therapeutic Goods Act, including those which relate to medical devices. The TGA is a Commonwealth body meaning that it has jurisdiction throughout the whole of Australia.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The role of the TGA in relation to digital health is multi-faceted and challenging. One of the primary roles of the TGA is determining whether a given digital health development meets the definition of a medical device – that is, when the legal manufacturer intends for the product to be used for: diagnosis; prevention; monitoring; treatment; or alleviation, of disease, injury or disability. If the device falls within the definition of a medical device the TGA must then classify it for inclusion in the ARTG.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

In early 2019, the TGA issued a Consultation paper on how software, including software as a medical device, should be regulated in Australia.

This consultation focused on proposed regulatory reforms that include introducing rules to classify software according to its potential to cause harm through the provision of incorrect information, ensuring that software products that are downloaded from overseas suppliers have an Australian sponsor who is responsible for the product in the Australian market, and clarifying the essential principles for safety and performance for medical devices that incorporate, or that are, software.

There was broad support for the three proposed reforms from the 41 submissions received.

After analysing the feedback from the consultation paper, the TGA held a workshop with stakeholders. The key outcomes of the workshop reinforced the consultation results for regulation to continue to be risk- and principles-based and internationally harmonised; there should be some Essential Principles specific to software; the boundary for regulated software should be clear; and there may be some products that could or should be expressly excluded from regulation.

The TGA has stated that it is continuing to work in this area, especially in relation to clearly defining the boundary between software products that are, are not, or should not be, included in the regulatory framework. Additional consultation will be conducted in 2020.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Health services (public and private) are required by privacy laws to take all reasonable steps to protect the health information it holds from misuse, interference, loss, unauthorised access, modification or disclosure.
  This may, for example, mean that steps need to be taken to ensure the rooms in which the patient and the telehealth provider are exchanging private health information have restricted access for the duration of the consultation, and to ensure that the transmission systems are secure and reviewed on a regular basis.
- **Robotics**
  In the event that robots are deployed to carry out healthcare functions by using data and private health information issues around data management, privacy and cyber-security become of paramount importance.
  Issues relating to legal liability for malfunctioning robotics may also present difficult problems.
- **Wearables**
  Wearable devices, such as pulse oximeters, are not automatically considered by the TGA to be medical devices. However, if claims are made in promotion, marketing or packaging such a device (whether expressly or impliedly) that it can be used for, or is suitable for, a therapeutic, diagnostic or monitoring function relative to a disease state, then the device would need to be registered on the ARTG as a medical device.
  Marketing and promotional claims for such devices must be considered objectively and disclaimers may be an important tool for manufacturers of such devices. The TGA may, however, assess the expected usage of such advice objectively, even in the presence of a disclaimer.
- **Virtual Assistants (e.g. Alexa)**
  As virtual assistant platforms evolve, consumers will be looking to leverage them to better manage their healthcare needs. This technology raises similar issues to telehealth – in particular, issues will arise around the management of patient privacy, data transfer and cybersecurity.
- **Mobile Apps**
  Many mobile apps are simply sources of information, or tools to manage a healthy lifestyle. The TGA does not regulate health and lifestyle apps and software that do not meet the definition of a medical device.
  Some mobile apps require the use of physical accessories that are connected to, or embedded in, the computing platform. These can be sensors that plug into a port on the platform, or features that are provided in the platform, such as speakers or a camera. This results in the combination of software, accessory and the computing platform becoming a medical device.
  One example is a glucose meter that reads blood test strips and plugs into a smartphone to display and store the results. In this case, the combination of meter, smartphone and app, is a medical device. The app is regulated as part of the glucose meter device.
  Some mobile apps can control or adjust a medical device through Bluetooth or WiFi features. These apps are considered to be software as a medical device because they are accessories to the medical device. They are regulated at the same risk classification level as the medical device they control.
- **Software as a Medical Device**
  The regulation of medical devices is risk-based. This means that the level of scrutiny and oversight by the TGA will vary according to the level of risk that the product represents to the patient or healthcare professional using it. The current regulations do not adequately capture all SaMD under the rules for this risk classification. The potential risks arising from SaMD products can be low, medium or high depending on the intended purpose of the SaMD. Regulatory reform in this area is underway and greater clarity should be available later in 2020 (see question 2.6 above).
  SaMD products must be included on the Australian Register of Therapeutic Goods (ARTG) before they can be supplied in Australia.
  The therapeutic goods legislation requires manufacturers of SaMD products (unless they are Class 1 – the lowest risk classification) to obtain Conformity Assessment certification to allow inclusion in the ARTG. All medical devices, irrespective of classification, are required to meet the Essential Principles for safety and performance.
- **AI-as-a-Service**
  In December 2019, the Australian federal government announced $7.5 million in funding for research into the

© Published and reproduced with kind permission by Global Legal Group Ltd, London

use of artificial intelligence (AI) in healthcare. It is hoped that the research will lead to improved clinical decision-making, new approaches in healthcare delivery and to help patients better manage their health.

Minister for Health, The Hon Greg Hunt MP, explained that AI will be critical in transforming the future of healthcare through improved preventative, diagnostic and treatment approaches.

AI-driven drug discovery is beginning to become mainstream in the pharmaceutical industry. Data and data collection techniques are the foundation for AI and, the greater the amount of data, the more informative the outcome. This has led to efforts by some pharmaceutical companies to combine their own data with those of competitors and run an external AI engine to generate better insights.

One major concern for pharma companies in sharing data among competitors is the perceived danger of letting external AI aggregators use their propriety datasets. One potential solution to this concern is federated learning which sends only limited aggregated datasets for analysis. Another approach is the use of virtual research environments that rely on anonymisation methods to enable privacy-aware collaborative analytics to be applied.

- **IoT and Connected Devices**

  Globally, the adoption of the IoT in the healthcare sector is increasing. Connected devices are being used for monitoring patient wellbeing, while others are being utilised for inventory management and workflow optimisation.

  A significant issue, however, is the increasing frequency of cyberattacks and ransomware. The secure integration of the IoT into medical devices and applications is a key concern. Solutions providers need to address these concerns by making regular firmware updates and secure protocols as the priority. In-home medical devices also pose an additional cybersecurity challenge.

- **Natural Language Processing**

  Natural language processing is among the fastest growing applications of artificial intelligence. NLP powers a growing number of tools, such as chatbots and virtual assistants like Amazon's Alexa.

  Challenges arise because to create a machine learning algorithm requires a machine to be "taught" how to interpret, distil and generate language almost spontaneously. That challenge is exacerbated in the case of NLP – software cannot pick up on subtlety. This is an acute problem in the case of healthcare applications where subtle changes of language may have serious consequences to a patient.

  True reliability and accuracy are a challenge, and certain problems such as word disambiguation and fragmented "doctor speak" can stump even the smartest NLP algorithms.

  Medical text is also often ungrammatical, with limited context. Clinical notes often use acronyms and abbreviations and many have multiple meanings making them highly ambiguous, e.g. "cold" can refer to a disease, a temperature sensation, or an environmental condition.

3.2 What are the key issues for digital platform providers?

The key challenge for platform providers in Australia, at the time of publication in early 2020, is the unsettled nature of the regulatory environment applicable to digital healthcare technology. New regulations are due to be promulgated in Australia during 2020 that will hopefully clarify definitions and consequently the scope of the existing medical device framework, so far as digital health is concerned. Digital platform providers will need to carefully and regularly monitor developments to ensure compliance with the developing regulatory requirements. Some comfort can be taken from public statements which the TGA has made that international harmony in this area is critical. Australian developments are therefore likely to be in tune with, or at least not inconsistent with, those in Europe and the US.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Health information is regarded as one of the most sensitive types of personal information. As such there are very strict rules surrounding the collection, use and disclosure of such information in Australia.

4.2 How do such considerations change depending on the nature of the entities involved?

The Privacy Act regulates the handling of personal information by Australian Government agencies and some private sector organisations. State and territory public hospitals and other agencies, as well as some private businesses, are governed by state/territory regulation. Some states and territories have specific health-related privacy legislation, others have general privacy legislation that also applies to health-related information and others do not have specific privacy legislation but have other laws which protect privacy and confidentiality.

4.3 Which key regulatory requirements apply?

The principal Commonwealth legislation applicable is the Privacy Act 1988 (Cth), including the Australian Privacy Principles, the My Health Records Act 2012 (Cth) and the Healthcare Identifiers Act 2010 (Cth). Various State and territory legislation is also applicable, such as, in Victoria, the Health Records Act 2001 (Vic) and the Information Privacy Act 2000 (Vic). Privacy legislation also exists in the Australian Capital Territory and New South Wales specifically to regulate the handling of personal health information. The Northern Territory, Queensland and Tasmania have general privacy legislation, which is broader in application. Each of these also have their own "information privacy principles" or requirements to a similar effect. In South Australia and Western Australia there are no privacy regimes, however, privacy is protected in other ways.

4.4 Do the regulations define the scope of data use?

Health information must only be used or disclosed for the primary purpose for which it was collected, although such information may be used and disclosed for another purpose with the patient's consent.

Otherwise, health information may be used and disclosed in certain very limited purpose circumstances, such as: when the patient would reasonably expect the information to be used or disclosed for the particular purpose, and the purpose is directly related to the primary purpose of collection; where the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order; where it is unreasonable or

© Published and reproduced with kind permission by Global Legal Group Ltd, London

impracticable to obtain consent to the use or disclosure, and there is a reasonable belief the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety; if use or disclosure is necessary for research or the compilation of analysis of statistics, relevant to public health or public safety, and a number of other conditions are met; or to prevent a serious threat to the life, health or safety of a genetic relative, provided a number of conditions are met.

4.5 What are the key contractual considerations?

See question 8.4.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Under the Privacy Act (see question 4.3), sensitive human and personal data is not permitted to be shared in its original form. Personal information is sensitive when it directly identifies a person and accompanies specific types of information including health information, genetic information and biometric information. However, de-identified sensitive data can legally be shared.

5.2 How do such considerations change depending on the nature of the entities involved?

See question 4.2.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The Privacy Act defines de-identified information as that which is no longer about an identifiable individual or an individual who is reasonably identifiable. The Act defines "identification information" (being the information which must be removed) as:

(a) the individual's full name;
(b) an alias or previous name of the individual;
(c) the individual's date of birth;
(d) the individual's sex;
(e) the individual's current or last known address, and two previous addresses (if any);
(f) the name of the individual's current or last known employer; or
(g) if the individual holds a driver's licence – the individual's driver's licence number.

The actual process of de-identifying data is authorised under the Australian Privacy Principles as an exception to sensitive data use.

6 Intellectual Property

6.1 What is the scope of patent protection?

The primary legal tests for determining what is, and is not, deserving of patent protection are that the invention must be for a "manner of manufacture", it must be novel, inventive, and a sufficient disclosure of the invention must be made. The "manner of manufacture" test is a threshold test for patent eligibility. Digital health innovations often take the form of specific applications of abstract ideas and are often computer-implemented methods or systems. In Australia, the distinction between eligible and ineligible inventions rests upon determining whether what is being claimed comprises ineligible subject matter (e.g. an abstract idea, or a mere scheme) implemented generally *via* "conventional" or "generic" computer hardware and software systems or whether, additionally, there is some patentable ingenuity in the implementation itself.

6.2 What is the scope of copyright protection?

Copyright protects copyright works such as literary works and artistic works from unauthorised reproduction or adaptation. In essence, copyright protects the material form of the work but not the underlying idea. Computer programs are defined as literary works for the purposes of copyright law. Copyright therefore offers some protection for digital health innovations that are computer software-related. Copyright may also be a viable means of protecting the form of a database (but not the underlying data itself).

6.3 What is the scope of trade secret protection?

Trade secret protection may assist digital health innovators where patent protection is not available. Underlying algorithms and software may be protectable by trade secrets, as may proprietary databases or compilations. Innovations that are susceptible to reverse engineering, however, are not good subject matter for trade secret protection. Trade secret protection only extends to information that is truly confidential – it is therefore incumbent on innovators to do all they can to maintain proprietary information in confidence.

6.4 What are the typical results on academic technology transfer rules?

Many Australian universities have sophisticated technology transfer offices that deploy a wide range of technology transfer methodologies ranging from intellectual property licensing to incubating start-up and spin-off companies. One example is the University of Melbourne, where research has led to the creation of many start-up companies such as Synchron – a neural interface technology company based in Palo Alto, California, developing minimally-invasive technology for safe and rapid implantation of miniaturised electronic medical devices with broadband capability.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

See questions 6.1, 6.2 and 6.3.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

It is vitally important to provide a clear and unambiguous contractual framework dealing with the intellectual property rights which flow as a result of the collaboration which, in turn, has implications for compensation and potential royalty flows. Provision should also be made for liability sharing, product

© Published and reproduced with kind permission by Global Legal Group Ltd, London

recall and insurance. Timing is also important – contractual rights and obligations should be put in place before the collaboration occurs.

7.2 What considerations apply in agreements between health care and non-health care companies?

Non-healthcare companies which have little or no previous experience of the healthcare sector often do not fully appreciate the highly regulated and scrutinised environment in which healthcare companies operate. This makes it even more critical for contractual arrangements to be clearly drafted to explicitly cover responsibilities for compliance with specific health-related laws and regulations.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

The term "machine learning" has no universally accepted definition. Broadly, it refers to an algorithmic framework that can provide insights into data from which inferences can be drawn. Real-life digital health interventions incorporating machine learning can be useful and effective even if, at present, that role is only just beginning to be explored in a clinical setting. Certainly, the Australian Therapeutic Goods Administration has machine learning and its implications for healthcare, firmly on its radar.

8.2 How is training data licensed?

There are a number of challenges surrounding the licensing of data. There are analogies with the building of software assets where the concept of open source licensing has gained broad acceptance. Machine learning and AI systems require vast amounts of training data. However, most intellectual property regimes treat data differently to software, with the consequence that common OSI-approved licences do not work so well when applied to data. For example, licences almost always grant a right to "use", but what does this mean in the context of machine learning and AI? Similarly, there is often a distinction made in licences between commercial and non-commercial use – given the way machine learning and AI is developing, that distinction is often blurred. The same definitional problems surround the license of data for "research" – when does research become commercial? In order to overcome these difficulties, some data communities are developing tailor-made solutions in the form of Community Data Licence Agreements. There are two kinds of such licences: the CDLA-Sharing licence which ensures that downstream recipients are permitted to use and modify the data but are required to share those changes; and the CDLA-Permissive licence, by contrast, allows the recipients to use and modify the data without any corresponding obligation to share any such modifications.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

In Australia, generally only work created by humans can be made the subject of copyright. Copyright only protects original works and courts have interpreted originality as requiring a degree of human ingenuity. A problem arises where AI software creates work which had little or no input from a human. Courts in Australia have been reluctant to attribute copyright where the work was largely created by a computerised process. For example, in *Acohs Pty Ltd v Ucorp Pty Ltd* (2012) 201 FCR 173, the Full Federal Court found that data sheets created by a computer program were not subject to copyright because there was not a sufficiently involved human author.

Under the *Patents Act 1990* (Cth), the question as to whether a patent would be granted where the named inventor is autonomous artificial intelligence remains unclear.

Section 15(1) of the Patents Act provides that a patent may be granted to a "person" who is the "inventor", or a "person" who is entitled to have the patent assigned to them. "Inventor" is not defined in the Act and "person" is defined in the *Acts Interpretation Act 1901* (Cth) to be a "body politic or corporate as well as individual".

It would therefore seem to be the case that an inventor, or a person entitled to have a patent assigned to them, must either be a body politic, corporation or individual.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Data licensing brings its own unique issues to the fore. Some important considerations include:

The Licence Grant

A data licence agreement should clearly define what data is actually being licensed, how the data will be provided, updated or manipulated, how current the data will be, the format in which the data will be delivered and the manner of delivery.

Use

The licence should also define who is permitted to use the licensed data. Any restrictions on use should be consistent with the anticipated use of the data. In the case of corporations, the licence should state whether the data can be used by affiliates of the licensee. A right of sub-licence may also be important.

For companies operating in different geographical locations, care should be taken to ensure the licensed data can be stored, accessed and used in all such locations.

Careful thought should be given to whether the licence is to be non-exclusive, exclusive to the licensee or a sole licence, so that the licensor and the licensee but no other third party may use the data.

Purpose

If data is licensed for a specific purpose, the licensee should include in the licence all of the possible purposes for which the data may be used because dataflow is difficult to control and may find its way into other databases, where it could be used for un-licensed purposes.

Data Security

The licence should address the nature and sensitivity of the data to be provided, the steps the licensee is required to take to protect and maintain the data and the licensee's potential liability if a data breach occurs.

Disclaimers

Licensors often seek to disclaim any representation or warranty with respect to the completeness, accuracy, timeliness or utility of the licensed data. A sophisticated licensee may seek to dilute

© Published and reproduced with kind permission by Global Legal Group Ltd, London

absolute disclaimers of this kind by introducing a knowledge or materiality qualifier.

Rights

In the case of personal or sensitive data it is particularly important for the licensee to ensure that the licensor is lawfully able to grant the licensee all of the rights the licensee requires to use the data for the anticipated purposes and that there are warranties included in the licence to that effect.

Term and Termination

A finite licence term in the case of data may be problematic – it can be difficult to trace data or it may be inter-mingled with other data so it may not be actually possible for the licensee to stop using the data. If these circumstances are anticipated, it may be preferable for the licensee to negotiate a perpetual licence.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Any digital health innovation that causes injury or loss, or which is not of merchantable quality, is actionable. Liability may be sheeted home to the manufacturer or the sponsor of the relevant product (or both) for negligence or for contravention of the Australian Competition and Consumer Act 2010 (Cth). Liability may also arise under the Australian Consumer Law for misleading advertisements or representations made about the product.

So far as personal information is concerned, under the Notifiable Data Breaches (NDB) scheme, any organisation or agency the Privacy Act 1988 covers must notify affected individuals and the Office of the Australian Information Commissioner when a data breach is likely to result in serious harm to an individual whose personal information is involved.

A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

- a device with a customer's personal information is lost or stolen;
- a database with personal information is hacked; or
- personal information is mistakenly given to the wrong person.

The notification to individuals must include recommendations about the steps they should take in response to the data breach.

9.2 What cross-border considerations are there?

Cloud computing, AI and machine learning present unique cross-border legal issues. Although these issues are not limited to the healthcare sector, they are arguably of most impact in the sector given the serious ramifications which flow from a failure of such systems. In most instances, digital health innovations will require registration on the Australian Register of Therapeutic Goods. This, in turn, will require a local Australian domiciled sponsor. The sponsor will have legal responsibility for the product concerned even if the manufacturer has no Australian presence. This may help to reduce cross-border legal issues in the context of liability for defective products.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

At the present time in Australia, data security and privacy concerns, regulatory compliance, interoperability and infrastructure availability are all significant issues.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Undoubtedly, the key issue is gaining a detailed understanding of the global regulatory environment that pertains to the digital health innovation concerned. Regulatory requirements differ, often markedly, between jurisdictions. It is important to know your potential markets and how the laws in each of those markets may impact the marketability of the product. It should not be assumed that what works in one market will be even be viable in another.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

Potential investors in digital healthcare businesses need to carry out detailed and intense due diligence focusing on the precise nature of the innovation and the extent to which that innovation is protected or is capable of protection by intellectual property rights – particularly taking into account that the scope of protection is likely to differ between jurisdictions. Similarly, the regulatory environment in each of the potential jurisdictions in which the innovation is likely to be marketed, needs to be clearly understood.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Wayne Condon has over 40 years' legal experience in Australia and New Zealand. He has advised and represented many global and domestic life sciences companies in regulatory, intellectual property and competition law matters. In 2018, Mr Condon established Biopharmalex as a fiercely independent, specialist life sciences law firm.

Biopharmalex
PO Box 1292
Hawksburn
Victoria 3142
Australia

Tel: +61 419 599 209
Email: wayne.condon@biopharmalex.com.au
URL: www.biopharmalex.com.au

Biopharmalex is recognised as a leading specialist life sciences focused law firm with core competency and experience in regulatory, intellectual property and competition law issues in Australia and New Zealand.
www.biopharmalex.com.au

Biopharmalex

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Austria

Herbst Kinsky Rechtsanwälte GmbH

Dr. Sonja Hebenstreit

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no general definition of "digital health" in Austrian Law. The European Commission has suggested using the term "telehealth" as referring to health-related procedures and "telemedicine" as referring to treating people from a distance (see https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf, page 25).

1.2 What are the key emerging technologies in this area?

All stakeholders including the public sector acknowledge that data-driven digital healthcare will transform the provision of healthcare services. Key emerging technologies are, in particular, AI applications including machine learning, which can contribute, e.g., to earlier disease detection and more accurate diagnosis.

1.3 What are the core legal issues in health care IT?

The main legal issues in healthcare IT are: compliance with data protection (see sections 4 and 5); the technical requirements for telehealth (see GTelG 2012 in question 2.1); as well as the determination of whether a product qualifies as a medical device (see questions 2.1 and 3.1).

2 Regulatory

2.1 What are the core health care regulatory schemes?

The Austrian Physicians Act 1998, Federal Law Gazette I 169/1998, as last amended by the Federal Law Gazette I 105/2019, (*Ärztegesetz* 1988, ÄrzteG 1988) contains regulations on training and admission as a physician, regulations on the exercise of the profession (e.g. group practices), prohibitions of discrimination and regulations on the organisation of the self-administration of physicians (Medical Association). Section 3 ÄrzteG stipulates that medical advice may only be given by licensed physicians. Section 49 paragraph 2 ÄrzteG further stipulates that physicians shall practice their profession "personally and directly". This provision is regarded as not generally prohibiting telemedicine, i.e. the individual diagnosis and treatment from distance, without direct human contact. The Austrian Medical Association has stated that telemedicine might support the relation between physician and patient and the treatment process and that digital monitoring and online contact might be helpful for the diagnosis as well as for the therapy, but has emphasised that a clear legal framework is required for telemedicine services. Currently, no such specific legal framework is in place. In any case, physicians are obliged to comprehensively inform the patient and get the patient's informed consent (likewise) in the case of telemedicine, they need to be in full control of the patient's situation, and the tele health treatment must be for the patient's benefit.

In the context of the referral of patients through online platform operators, the prohibition of commissions according to Section 53 paragraph 2 ÄrzteG needs to be observed, according to which the physician may not promise, give, take or have promised to himself or another person any remuneration for the referral of patients to him or through him. According to paragraph 3 *leg cit*, activities prohibited under paragraph 2 are also prohibited for group practices (Section 52a) and other physical and legal persons. This means that the collection of commissions from patients is prohibited not only for doctors but also for other third natural or legal persons.

The Austrian Medicinal Products Act, Federal Law Gazette 185/1983, as last amended by Federal Law Gazette I 104/2019, (*Arzneimittelgesetz*, AMG) implements a large number of European Union directives concerning regulations on medicinal products, in particular Directive 2001/83/EC – Community code relating to medicinal products for human use. The AMG contains regulations on the authorisation of medicinal products, regulations regarding marketing, advertising and distribution of medicinal products as well as quality assurance requirements.

The Austrian Medical Devices Act, Federal Law Gazette 657/1996, as last amended by Federal Law Gazette I 100/2018, (*Medizinproduktegesetz*, MPG) implements a large number of European Union directives concerning medical devices, in particular Council Directive 93/42/EEC concerning medical devices. The Medical Device Regulation 2017/745 on medical devices (MDR) will repeal the MPG on May 26, 2020. The MDR lays down rules concerning the placing on the market, making available on the market or putting into service of medical devices for human use and accessories for such devices in the Union. The MDR shall also apply to clinical investigations concerning such medical devices and accessories conducted in the European Union.

2.2 What other regulatory schemes apply to digital health and health care IT?

The General Data Protection Regulation, Regulation 2016/679 (GDPR) contains central provisions on data protection.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Although the GDPR as a regulation applies uniformly and directly throughout the European Union, a large number of opening clauses allow national deviations by the member states. Providers of digital health and healthcare IT in particular need to take into account the provisions on the lawfulness of the processing of health data pursuant to Article 9 GDPR as well as the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk pursuant to Article 32 GDPR.

The Austrian Data Protection Act, Federal Law Gazette I 165/1999, as last amended by Federal Law Gazette I 14/2019, (*Datenschutzgesetz*, DSG) specifies the provisions of the GDPR and, in particular, contains provisions on proceedings before the Austrian data protection authority. For the private sector, the DSG does not provide any provisions for the processing of health data that deviate from the GDPR.

The Austrian Health Telematics Act 2012 (*Gesundheitstelematikgesetz 2012*, GTelG 2012) contains special regulations for the electronic processing of health data and genetic data (please refer to Article 4 No. 15 and 13 GDPR) by healthcare providers. A healthcare provider in the meaning of health telematics is a professional who, as a controller or processor (in the meaning of Article 4 Nos. 7 and 8 GDPR), regularly processes health data or genetic data in electronic form for the following purposes:

- medical treatment or care;
- nursing care;
- invoicing of health services;
- insurance of health risks; or
- exercise of patient rights.

The GTelG 2012 also contains detailed regulations on the operation of the Electronic Health Record (*Elektronische Gesundheitsakte*, ELGA) by ELGA GmbH, which is owned by the Republic of Austria, the Main Association of Austrian Social Insurance Institutions and the federal provinces or their health funds.

2.3 What regulatory schemes apply to consumer devices in particular?

The Medical Devices Act and, as of May 2020, the Medical Devices Regulation (see question 2.1) likewise apply to Consumer Devices.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

In connection with GTelG 2012 and GTelV 2013, the Federal Minister for Health is competent for notifications and for the operation of the eHealth directory service according to paragraphs 9 and 10 GTelG 2012.

In connection with the ÄrzteG, the competent authorities are the Austrian Medical Chamber, the respective state governor ("*Landeshauptmann*") and the Federal Minister for Health.

The Federal Office for Safety in Health Care (*Bundesamt für Sicherheit im Gesundheitswesen*, BASG) is the central regulatory authority for the medicinal products and medical devices industry. The BASG is responsible, among other things, for the approval of medicinal products, market surveillance and pharmacovigilance, notifications in connection with clinical trials, the control of advertising restrictions and the granting and review of operating licences.

Investigations and assessments are typically carried out by the Austrian Agency for Health and Food Safety (*Österreichische Agentur für Gesundheit und Ernährung*, AGES) on behalf of the BASG.

The Austrian Data Protection Authority (*Datenschutzbehörde*, DSB) is the supervisory authority in Article 4 Section 21 GDPR, for the monitoring of data protection law and the assertion of data subjects' rights under the GDPR.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

As far as can be seen, neither the Austrian Medical Chamber nor the BASG or the Federal Minister of Health recently took relevant enforcement measures in the regulatory area of digital health and healthcare IT.

The DSB recently rendered a major decision regarding the communication between physicians and patients (DSB-D213.692/0001-DSB/2018): according to the DSB, patients cannot consent to the (unencrypted) transmission of health data (e.g. medical reports) by physicians. The DSB reasoned that the choice of the communication method is a technical/organisational measure according to Article 32 GDPR, and that no consent can be provided to insufficient technical/organisational measures.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

According to Recital 19 MDR, software qualifies as a medical device, when specifically intended by the manufacturer to be used for one or more medical purposes, while software for general purposes, even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device. The qualification of software, as either a device or an accessory, is independent of the software's location or the type of interconnection between the software and a device. Therefore, as a general rule, software for general purposes, even if used in the healthcare sector, is not a medical device. The manufacturer determines the intended use which is essential for software for general purposes to be differentiated from a medical device.

According to the MDR, manufacturers of medical devices are obliged to carry out a clinical evaluation for all their products – regardless of the risk class – which also includes a post-market clinical follow-up (PMCF). Such clinical evaluation is an essential task of the manufacturer and an integral part of a manufacturer's quality management system (Article 10 paragraphs 3 and 9f MDR). The clinical evaluation is a systematic and planned process for the continuous generation, collection, analysis and evaluation of clinical data for a device. Through the clinical evaluation, the manufacturer verifies the safety and performance of his device, including the clinical benefit.

Furthermore, Regulation No. 207/2012 on electronic instructions for use of medical devices must be observed when providing electronic instructions for use.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  According to Section 3 ÄrzteG, medical advice may only be given by licensed physicians. Furthermore, the physician needs to decide in each individual case of such telehealth consultation if he/she can sufficiently control

© Published and reproduced with kind permission by Global Legal Group Ltd, London

possible dangers despite the lack of physical contact with the patient and whether he/she has a sufficient information basis for his/her decisions. In case the physician has to fear that he/she does not have a sufficient basis for his/her medical decision due to lack of physical patient contact, he/she must advise the patient to actually (physically) see a physician.

Austrian law does not contain rules for the provision of telehealth or telemedicine services in general, but a specific regulation has been issued regarding the provision of teleradiology services: the Medical Radiation Protection Regulation (BGBl II Nr 375/2017) provides that teleradiology is permitted within the framework of basic and special trauma care as well as in dispersed outpatient primary care facilities of acute hospitals and otherwise only in order to maintain night, weekend and holiday operations for urgent cases.

According to paragraphs 3 and 4 of the GTelG 2012, health service providers may transfer health data and genetic data only if:

- the transmission is permitted under Article 9 GDPR;
- the identity of those persons whose health data or genetic data are to be transmitted is proven;
- the identity of the healthcare providers involved in the transmission is proven;
- the roles of the healthcare providers involved in the transmission are demonstrated;
- the confidentiality of the transmitted health data and genetic data is guaranteed; and
- the integrity of the transmitted health data and genetic data is guaranteed.

In addition, the GTelG 2012 and the Health Telematics Regulation 2013, Federal Law Gazette II 506/2013, (*Gesundheitstelematikverordnung 2013*, GTelV 2013) issued by the Federal Minister of Health on the basis of GTelG 2012 contain detailed regulations on encryption and technical implementation of communication.

- **Robotics**
  According to Section 3 ÄrzteG, medical advice may only be given by licensed physicians. Furthermore, robotics may be subject to MDR when specifically intended by the manufacturer to be used for one or more medical purposes (e.g. robotics for surgical purposes).
- **Wearables**
  Wearables may be subject to MDR when specifically intended by the manufacturer to be used for one or more medical purposes.
- **Virtual Assistants (e.g. Alexa)**
  According to Section 3 ÄrzteG, medical advice may only be given by licensed physicians. Virtual Assistants in general would not qualify as a medical device. However, natural language processing may be subject to MDR when specifically intended by the manufacturer to be used for one or more medical purposes.
- **Mobile Apps**
  See question 2.6 (Software as a Medical Device).
- **Software as a Medical Device**
  See question 2.6.
- **AI-as-a-Service**
  See question 2.6 (Software as a Medical Device) and section 8 (AI and Machine Learning).
- **IoT and Connected Devices**
  IoT and Connected Devices may be subject to MDR when specifically intended by the manufacturer to be used for one or more medical purposes (e.g. blood pressure measurement using cloud recording).
- **Natural Language Processing**
  Natural Language Processing generally does not qualify as a medical product (e.g. speech recognition in dictation software). However, Natural Language Processing may be subject to MDR when specifically intended by the manufacturer to be used for one or more medical purposes.

3.2 What are the key issues for digital platform providers?

One of the main restrictions on digital platforms for individual healthcare is that medical advice may only be given by licensed physicians (Section 3 ÄrzteG; see question 2.1).

Furthermore, online platform operators should keep in mind the prohibition of commissions in Section 53 paragraph 2 ÄrzteG, according to which the physician may not promise, give, take or have promised to himself or another person any remuneration for the referral of patients to him or through him. Moreover, these activities are also prohibited for group practices (Section 52a) and other physical and legal persons. This means that the collection of commissions from patients is prohibited not only for doctors, but also for other third (natural or legal) persons.

Moreover, digital platforms must take appropriately (high) technical/organisational measures for data security when processing health data (Article 32 GDPR).

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The processing of personal data must comply with the GDPR. When processing health data, Article 9 GDPR applies; according to that provision, the processing of health data in connection with healthcare providers is lawful only if (only the most relevant legal grounds have been included in the following):

- the data subject has given explicit consent to the processing of their personal data for one or more specified purposes (Article 9 Section 2 letter a GDPR);
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (Article 9 Section 2 letter c GDPR);
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems (Article 9 Section 2 letter h GDPR);
- pursuant to a contract with a health professional, when the data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy (Article 9 Section 2 letter h in connection with Section 3 GDPR); and
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices (Article 9 Section 2 letter i GDPR).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

4.2 How do such considerations change depending on the nature of the entities involved?

In principle, the provisions of the GDPR apply equally to all entities. However, the legal grounds in Article 9 Section 2 letter h only apply to data processing, when the data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy. Therefore, entities not subject to professional secrecy cannot rely on this legal ground.

4.3 Which key regulatory requirements apply?

The general regulatory provisions of the GDPR apply.

4.4 Do the regulations define the scope of data use?

Yes, please refer to question 4.1. Some legal grounds of Article 9 impose limitations on the purpose of the processing (e.g. preventive or occupational medicine; see question 4.1).

4.5 What are the key contractual considerations?

If the processing is based on explicit consent of the data subject, such valid and fully informed consent needs to be given by the patient. Furthermore, according to Article 28 GDPR, any data controller must conclude a written data processing agreement with processors, which must contain the minimum contents specified therein.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Sharing health data between healthcare professionals is subject to the GTelG 2012 (see question 3.1 for the conditions of sharing under the GTelG 2012), sharing of data between individuals other than healthcare professionals is solely subject to the GDPR; see question 4.1 for sharing within the EU. For sharing with an individual located outside the EU/EEA, the GDPR provisions on the transfers of personal data to third countries or international organisations apply.

5.2 How do such considerations change depending on the nature of the entities involved?

Sharing of data between individuals other than healthcare professionals is solely subject to the GDPR (see question 4.1). In this case GTelG 2012 does not apply.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please refer to question 4.3.

6 Intellectual Property

6.1 What is the scope of patent protection?

Technical inventions which are novel, which, considering the state of the art, are not obvious to a person skilled in the art, and which can be applied in the industry can be subject to patent protection under the Austrian Patent Act, BGBl. Nr. 259/1970, as last amended by BGBl. I Nr. 37/2018. Only a natural person can qualify as an inventor.

The inventor can either file a patent himself or transfer his right to a third party. The patent owner has the exclusive right to manufacture, put into circulation, offer for sale and use the patented invention for the duration of the patent, namely up to 20 years. A "prolongation" of the patent protection can only be achieved by virtue of a Supplementary Protection Certificate, a *sui generis* intellectual property right available for specific medicines and plant protection products.

6.2 What is the scope of copyright protection?

Under Austrian law (the Austrian Federal Law on Copyright in Works of Literature and Art and on Neighbouring Rights, Federal Law Gazette (BGBl) 1936/111 as last amended by BGBl I 150/2013 – *Urheberrechtsgesetz* – UrhG), a work is defined as an "original intellectual creation" (Section 1 paragraph 1 UrhG). The author has the exclusive right to use his or her work in the way defined by the law (in particular reproduction right, distribution right, rental and lending right, broadcasting right, right of public performance and of communication to the public of a performance, making available right). Protection starts in the very moment of creation, which means that no registration with any authority is required for protection under the Copyright Act. According to Section 1 paragraph 1 UrhG, works can be original intellectual creations in the area of literature (including computer programs), musical arts, visual arts and cinematography. In principle, only creations of human beings are regarded as works and protected by copyright and the legislator has so far not provided for specific rules for "computer generated works". According to current doctrine, computer generated works might still be subject to copyright protection and the programmer as the author in case the programmer, although not directly involved in the creation of the work, has created the creative framework for it by programming the appropriate autonomy.

The Copyright Act further grants exclusive rights to performers (such as singers, dancers and actors) as well as phonogram producers, photographers, broadcasters and the producers of a database (*sui generis* right).

6.3 What is the scope of trade secret protection?

The UWG contains in its Sections 26a *et seq.* the Unfair Competition Act ("UWG") civil law and civil procedural law rules for the protection of trade secrets. According to the legal definition in Section 26b UWG, information that is:

- secret, namely not known or readily accessible by persons that normally deal with the respective information;
- of commercial value because of its secrecy; and
- subject to reasonable measures to be kept secret,

qualifies as a trade secret.

It must be proven that *reasonable measures* have been taken; these may include specific IT security measures and the restricted accessibility of secret information (e.g. only accessible to particularly trustworthy employees).

A variety of information may be regarded as a trade secret, for example, inventions and designs (if not protected as a patent or design) as well as not otherwise protected information such as production processes, customer information, business models or the like.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

The owner of a trade secret is particularly entitled to claims of forbearance, removal, and damages against anyone who unlawfully acquires, uses or discloses his trade secrets.

Section 26h UWG contains specific rules to ensure the protection of trade secrets in civil proceedings.

6.4 What are the typical results on academic technology transfer rules?

Universities may claim any service invention made by one of its employees within three months of notification of the invention (see Section 106 paragraph 2 University Act (*Universitätsgesetz* – UG) in connection with the Patent Act's rules on service inventions); the employee is generally entitled to a special remuneration if the university makes use of that right. If the university does not claim the invention, the general rule applies, namely, the inventor is entitled to the invention. Regarding the commercialisation of technology developed by its researchers, Austrian universities pursue different strategies – from outlicensing to transferring IP and increasingly, additionally acquiring shares in its spin-out companies.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

There are no specific rules for Software as a Medical Device from an intellectual property protection point of view, i.e. the software will be protected by copyright law and might eventually also be patentable.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

If not otherwise regulated, collaborative improvements belong to the respective inventors of such improvement, whereas the ownership of the basis technology will not change following such improvements. The ownership, and eventually licences regarding the use of such collaborative improvements, is therefore usually regulated precisely and meticulously in the respective agreements containing the regularities for the collaboration.

7.2 What considerations apply in agreements between health care and non-health care companies?

Besides regulatory considerations (see in particular question 2.1), the general principles apply, namely Austrian law's (federal) rules on commercial contracts, providing regulations on the general principles and specific contract types.

The general principles of contracts as well as a large number of specific contracts are regulated in the Civil Code (*Allgemeines Bürgerliches Gesetzbuch*) and in the Commercial Code (*Unternehmensgesetzbuch*).

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Many digital health devices use machine learning (such as, e.g., in the field of radiology, and generally in diagnosing). Machine learning is substantial for developing smart digital health solutions and is said to have the potential to substantially transform healthcare both for patients and medical professionals.

8.2 How is training data licensed?

The protection and licensing of training data does not differ from any other protection of information, creations and data. If the training data were created in a specific way by a human being (e.g., texts for speech recognition) they may be subject to copyright protection (see question 6.2). In addition, training data may also be subject to trade secrecy protection (see question 6.3).

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Software may in principle be protected by copyright (see question 6.2). However, copyright protection presupposes an "intellectual creation" which, according to Austrian law, can only originate from the thoughts of a human being. Assuming that the improvement could have only been achieved because the programmer has "instructed" the algorithms correspondingly, it could be argued that the programmer is the author of the work (the improvement, which is furthermore depending on the basis work). In case the improvement was indeed created without active human involvement it does not qualify for copyright protection.

8.4 What commercial considerations apply to licensing data for use in machine learning?

For the provision of data for use in machine learning, the licensor is often commercially interested not only in remuneration but will often have an interest in technical cooperation under which the licensor acquires rights to the results of the machine learning. Therefore, the provision of data for use in machine learning is often based on a broad cooperation.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Austrian tort law generally stipulates that the tortfeasor is obliged to compensate for those damages which he or she has culpably and unlawfully caused. In addition to material damages, the injured party is also entitled to receive compensation for pain and suffering in case of injuries to the body and/or health. Punitive damages are not paid in Austria. Unlawfulness in the context of the provision of health services typically results from the violation of contractual obligations (e.g. duties of care, non-valid consent to the treatment because of incorrect or insufficient information). The liability for personal injury cannot be excluded and/or limited by contract.

The Austrian Product Liability Act, Federal Law Gazette 99/1988, last amended by Federal Law Gazette I 98/2001, (*Produkthaftungsgesetz*, PHG) transposes in particular Directive 1999/34/EC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. If a defect in a product kills a

© Published and reproduced with kind permission by Global Legal Group Ltd, London

person, causes bodily injury or damage to health, or damages a physical object other than the product, the manufacturer, distributor and the importer shall be liable for damages under Section 1 PHG. Liability is subject to the product being defective and therefore not offering the safety that can be expected under consideration of all circumstances (Section 5 paragraph 1 PHG). However, liability shall be excluded if the manufacturer, distributor or importer proves that: (i) the defect is due to a legal provision or official order with which the product had to comply; (ii) the characteristics of the product are in accordance with the state of the art in science and technology at the time when the person making the claim put it into circulation; or (iii) where the person claimed has manufactured only one basic material or part of a product, the defect was caused by the design of the product into which the basic material or part has been incorporated or by the instructions of the manufacturer of that product.

9.2 What cross-border considerations are there?

In case it is intended that foreign doctors provide telemedical treatment to Austrian patients, these require an Austrian professional licence if their activity does not fall under Section 37 ÄrzteG (freedom to provide services). According to Section 37 ÄrzteG, nationals of EU or EEA Member States or Switzerland who lawfully exercise the medical profession in another EU/EEA Member State or Switzerland may, from their foreign professional domicile or place of employment, practise medicine in Austria only if the medical activity is temporary and occasional, which must be assessed on a case-by-case basis, in particular on the basis of the duration, frequency, regular return and continuity of the activity.

Further considerations refer to the law applicable in a cross-border scenario: the provision of health services is typically based on a contract concluded by a natural person for a purpose which can be regarded as being outside his trade or profession (the patient) with another person acting in the exercise of his trade or profession (the medical professional). According to Article 6 Regulation 593/2008 on the law applicable to contractual obligations (Rome I) the contract as well as the contractual liability derived therefrom shall therefore be governed by the law of the country where the consumer has his habitual residence, provided that the professional: (i) pursues his commercial or professional activities in the country where the consumer has his habitual residence; or (ii) by any means, directs such activities to that country or to several countries including that country. Cross-border healthcare providers therefore typically have to comply with the laws of a large number of countries in which they offer their services.

For claims arising from product liability under the PHG, pursuant to Article 5 Regulation 864/2007 on the law applicable to non-contractual obligations (Rome II), the law applicable shall be: (i) the law of the country in which the person sustaining the damage had his or her habitual residence when the damage occurred, if the product was marketed in that country; or, failing that; (ii) the law of the country in which the product was acquired, if the product was marketed in that country; or, failing that, (iii) the law of the country in which the damage occurred, if the product was marketed in that country. As a result, providers of medical devices must therefore also comply with a large number of legal systems in the area of product liability.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Like for healthcare IT in general (see question 1.3) the main legal issues for cloud-based services for digital health are the compliance with data protection (see sections 4 and 5), the technical requirements for telehealth (see GTelG 2012 in question 2.1) as well as determining whether a product qualifies as a medical device (see questions 2.1 and 3.1).

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

The intended business model and the actual product or service that shall be offered needs to be carefully examined from a legal perspective, in particular from a regulatory (e.g., the Physicians Act and limitations of telemedicine, Medical Devices Regulation) and from a data protection point of view. Furthermore, if such is relevant depending on the business model, it should be assessed whether reimbursement of the services in question by the sick funds is at all possible.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

A comprehensive regulatory (including data protection) due diligence is advisable in order to safeguard that the business the digital healthcare venture intends to undertake or already undertakes complies with all applicable legal requirements.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Dr. Sonja Hebenstreit is a Partner at Herbst Kinsky Rechtsanwälte GmbH, which she joined in 2005. She specialises in the fields of intellectual and industrial property law, unfair competition, life sciences, data protection as well as antitrust and competition law. Dr. Sonja Hebenstreit is a certified data protection officer.

Education and Career: *Mag. iur.* (Vienna 1997); *Dr. iur.* (Vienna 2001); internships with the European Commission (Brussels 1998) and British Telecommunications Group, Legal Services (Brussels 1999); researcher at the University of Münster (Germany), ITM/Civil Law Department (1999–2000); law practice with Hausmaninger Herbst Attorneys at Law (2000–2005); and Herbst Kinsky Rechtsanwälte GmbH (since 2005). Admitted to the Austrian Bar (Vienna 2003).

Languages: German; English; and French.

Herbst Kinsky Rechtsanwälte GmbH
Dr. Karl Lueger-Platz 5
A-1010 Vienna
Austria

Tel: +43 1 904 2180 161
Fax: +43 1 904 2180 210
Email: sonja.hebenstreit@herbstkinsky.at
URL: www.herbstkinsky.at

The Firm

Since its establishment in 2005, Herbst Kinsky has become one of Austria's leading commercial law firms. Its specialised and highly committed lawyers combine many years of experience gained abroad and in reputable Austrian law firms. The firm's practice covers a full range of services in all areas of commercial, corporate, civil and public law, including banking, insurance and capital markets, corporate and M&A, IP, IT and life sciences, merger control, antitrust and competition, data protection, real estate, dispute resolution and arbitration.

Our Clients

The firm's clients range from large international privately-held and publicly-listed companies, banks, insurance companies and private equity investors to small and mid-size business entities. Clients cut across many different industries, including life sciences, energy, information technology, financial institutions and insurance.

www.herbstkinsky.at

HERBST KINSKY
RECHTSANWÄLTE GMBH

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Belgium


Olivier Van Obberghen


Pieter Wyckmans


Amber Cockx

Quinz

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

Digital health or e-health stands for the use of information and communication technologies (ICT) – and in particular internet technology – to support or improve healthcare.

1.2 What are the key emerging technologies in this area?

Currently, technologies improving personalised and preventive care are gaining ground. Telemonitoring by means of apps, wearables and other medical devices permit early detection, while personalised care facilitates the optimal use of healthcare's limited resources to maximise patient benefits.

1.3 What are the core legal issues in health care IT?

The emergence of new health technologies results in changing roles for healthcare actors and challenges the boundaries of the current legal framework. Patients no longer merely undergo treatment but are empowered to take an active role in the co-maintenance of their own health. Telehealth changes the role of the hospital and its personnel into one of surveillance, shifting from inpatient to outpatient treatment. Accordingly, competition between hospitals becomes greater, as patients are no longer limited to making use of the services of the nearest hospital. Lastly, the medical (devices) industry may come into direct contact with patients (e.g. through providing information) and a patient's personal data may be processed by the industry before the healthcare professional receives such data, resulting in concerns regarding data protection and illegal promotion of health products.

2 Regulatory

2.1 What are the core health care regulatory schemes?

- Act on the Performance of the Healthcare Professions of 10 May 2015.
- Act on Hospitals and Other Care Facilities of 10 July 2008.
- Patients' Rights Act of 22 August 2002.
- Law on Medicines of 25 March 1964.
- EU Regulation 2017/745 on Medical Devices and Law on Medical Devices of 15 December 2010.
- Law on Experiments with Humans of 7 May 2004.
- Code of Medical Ethics of the Belgian Medical Association.

2.2 What other regulatory schemes apply to digital health and health care IT?

The legislation on product liability, data protection and e-commerce is relevant to digital health and healthcare IT. General regulations on competition, consumer law and unfair commercial practices must also be kept in mind. Finally, specific rules, e.g. on the Belgian e-health platform or the EU framework on cross-border healthcare, must be consulted.

2.3 What regulatory schemes apply to consumer devices in particular?

The legislation on medical devices, product liability, e-commerce and the consumer protections set forth in the Code of Economic Law are relevant to consumer devices.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

First, the Belgian National Institute for Health and Disability Insurance (NIHDI) is responsible for establishing reimbursement schemes for healthcare services, health products and medicines. Further, the Federal Agency for Medicines and Health Products (FAMHP) supervises the quality, safety and efficacy of medicines and health products. Also, professional associations such as the Order of Physicians and the Order of Pharmacists regulate the deontological aspects of healthcare professions. The Belgian Data Protection Authority (DPA) enforces compliance with data protection.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The DPA and the Market Court in Brussels ensure enforcement of data protection infringements. In addition, the FAMHP can take administrative sanctions and restrict the placing of medicines and health products on the market.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

If software is considered a medical device (for more information on this classification, see question 3.1), EU Regulation 2017/745 on Medical Devices and/or EU Regulation 2017/746 on *In Vitro* Diagnostic Medical Devices may apply, depending on the type of medical device. Medical devices must undergo a conformity assessment and must be certified and CE marked before being placed on the market.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Up until recently, the National Council of the Order of Physicians required the presence of both the physician and the patient in the same place for the diagnosis of patients. Telemonitoring or tele-expertise between physicians where no diagnosis was made did not have to fulfil this criterion and could be performed at distance. Since September 2019, the diagnosis of patients at distance has been allowed if the physician knows the patient, has his/her medical records, and can guarantee the continuity of healthcare provision. It is thus still impossible to have a first encounter with a patient over the internet. Another concern is the reimbursement of telehealth services. Currently, telehealth services are not part of the nomenclature of the Belgian National Institute for Health and Disability Insurance (NIHDI) and are therefore not reimbursable. The NIHDI is currently working on a regulatory framework for reimbursement.
- **Robotics**
  Robotics are currently widely used in surgery across Belgium. The traditional rules regarding contractual, extracontractual, medical and product liability apply (see question 9.1 below), but given the different actors involved (the manufacturer, importer, supplier, physician, hospital, etc.) it may be difficult for a patient suffering damage due to robot-assisted surgery to assess the most suitable remedy for her/his claim. Concerns have also been raised regarding the limited competition amongst manufacturers supplying Belgian hospitals with robot technology.
- **Wearables**
  Telemonitoring through wearables experiences similar difficulties as telehealth in general. Reimbursement schemes are limited to a few specific wearables classified as a medical device but are non-existent for others. In this regard, wearables are subject to considerably different regulatory frameworks based on the classification as a medical device or not. This classification as a medical device is based upon whether the instrument, appliance, software, etc. is intended to be used for one of the medical purposes in art. 2(1) of EU Regulation 2017/745 on Medical Devices. The medical devices framework is far more burdensome and manufacturers have an incentive to indicate/claim that their health product is not intended to be used for one of these medical purposes in order to avoid having to comply with EU Regulation 2017/745 on Medical Devices.
- **Virtual Assistants (e.g. Alexa)**
  Speech recognition devices are widely used by healthcare professionals to document information on to patient health records. In addition, virtual assistants are particularly interesting for personalised care and the increasingly older population in Belgium. Besides cybersecurity issues, the storage of information counter to the "storage limit principle" of the EU's General Data Protection Regulation (GDPR) might raise data protection concerns.
- **Mobile Apps**
  The main concerns regarding mobile apps are still privacy and data protection considerations. The GDPR demands transparency and informed consent for a specific purpose, however, in practice, users of mobile health apps are scarcely aware for which purposes their data are used. Despite establishing a "purpose limitation principle", the GDPR provides some leeway for further processing of data if compatible with the initial purpose of data processing. In addition, if mobile health apps are used in healthcare and prescribed by a healthcare professional, patients that are not on the internet may not be discriminated. Also, the patient's rights under the Patients' Rights Act need to be respected, such as the right to quality healthcare. Again, reimbursement is lacking for mobile health apps, although steps have been taken to remedy this issue (see, for example the MHealth Belgium website).
- **Software as a Medical Device**
  The classification of software as a medical device suffers from the same shortcomings as the ones for wearables. Software will be considered a medical device if it is intended by its manufacturer to have a medical purpose or if the software meets the definition of an "accessory" for a medical device. As said, the classification as a medical device has consequences for the regulatory framework that applies to software. In addition, (software as) a medical device is liable to cybersecurity breaches. The applicable medical devices legislation does not provide for specific safeguards regarding cybersecurity.
- **AI-as-a-Service**
  If the entity delivering AI-as-a-Service is collecting (big) personal data and the data can be linked to a data subject (not anonymised), the GDPR applies. The processing of personal data has to be compatible with the purpose limitation principle and the principle of data minimisation; the relevant personal data need to be correct (which may be specifically relevant in a big data analysis context) and the rights of the data subject need to be respected. If the service is performed outside the EU/EEA, specific data protection safeguards apply.
- **IoT and Connected Devices**
  Again, while the IoT and connected devices offer great advantages for patients (e.g. assisted living), for physicians (e.g. telemonitoring), and for hospitals (e.g. stock management and patient identification), privacy, data protection and security issues have been raised.
- **Natural Language Processing**
  When NLP software processes personal data, it needs to comply with the GDPR. Other privacy and security concerns may also arise.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

3.2 What are the key issues for digital platform providers?

The liability of digital platform providers for copyright breaches and other infringements has been limited (Book XII of the Code of Economic Law). Hosting providers cannot be held liable for infringements committed through their services insofar as the service provided merely consists of the storage of information provided by a recipient of the service. In addition, the platform provider may not have (had) knowledge of the illegal activity or information. Once the provider has actual knowledge of the infringement, it needs to act expeditiously to remove or to disable access to the information concerned and it needs to inform the public prosecutor of such infringement. The e-health platform used by physicians is regulated in a separate law (Law on the Establishment and Organisation of the eHealth Platform and Miscellaneous Provisions of 21 August 2008). One also needs to contemplate competition rules when collaborating on digital platforms, e.g. the exchange of (sensitive) information between independent healthcare practitioners.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

As in most jurisdictions, the use and processing of personal data in healthcare in Belgium has drastically changed over the last decades. In the past, a patient's medical records were usually stored by her/his treating physician in a paper version and were solely used for the purposes of treatment. With the introduction of e-health, other actors have entered the process, resulting in greater risks of privacy and/or data protection breaches. Under the GDPR and under the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data, data related to health are considered as sensitive data. In principle, such data cannot be processed unless an exception applies, e.g. informed consent, medical diagnosis by someone under the obligation of professional secrecy, reasons of public interest in the area of public health, etc. (art. 9 GDPR). The right to privacy (art. 8 European Convention of Human Rights, art. 7 Charter of the EU and art. 22 of the Constitution) and the right to data protection (art. 8 of the Charter of the EU, art. 16 Treaty on the Functioning of the EU and art. 10 Act on Patients' Rights) of a patient need to be reconciled with the advantages of the processing and sharing of certain medical data. On an individual basis, electronic health records and the automatic processing of personal data may facilitate long-term follow-up by several different healthcare providers. On a larger scale, (big) data analyses of personal data may increase the quality and efficiency of healthcare, offer predictive therapeutic models and allow for personalised care of patients.

4.2 How do such considerations change depending on the nature of the entities involved?

As a consequence of the introduction of e-health, the personal data of patients are no longer solely processed by physicians and other healthcare providers, who are bound by professional secrecy on penalty of criminal sanctions under art. 458 of the Criminal Code (art. 25 Code of Medical Ethics of the Belgian Medical Association). Employees of the medical devices industry or health app providers may be in direct contact with patients and process their personal data. Under the GDPR, one may only process personal health-related data when one of the grounds of art. 9.2 applies. Personal data may be processed for purposes of preventive or occupational medicine, medical diagnosis or the provision of health or social care treatment, but this may only be done under the responsibility of a professional subject to the obligation of professional secrecy (art. 9.2(h) and art. 9.3 GDPR). Accordingly, health app providers may not benefit from this provision and must obtain informed consent in order to be allowed to process personal data (art. 9.2(a) GDPR).

4.3 Which key regulatory requirements apply?

In the physician-patient relationship, patients have the right to consult their medical record, which should be updated and stored carefully (art. 10 Act on Patients' Rights and art. 22–24 Code of Medical Ethics of the Belgian Medical Association). Since 2008, a national e-Health platform has been established, where healthcare providers upload electronic health records of a patient after having obtained the patient's consent (art. 5.4(b) Law Establishing and Organising the eHealth Platform). Only healthcare providers having a therapeutic relation with the patient may access the electronic health records of a patient, excluding, for example, medical advisors from insurance companies. In the broader context of (e-)health services, one must take account of the GDPR and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data. Health-related data may only be processed lawfully, fairly and in a transparent manner. It may only be collected for specific, explicit and legitimate purposes and must be minimised to what is strictly necessary for the purpose. Personal data must be accurate and anonymised as far as possible and securely processed. For health-related data, one of the grounds of art. 9.2 GDPR must be fulfilled to permit data processing. The controller, which may be a doctor or a hospital, safeguards these principles. Additionally, a data protection officer must be appointed when the main activity of a controller or processor is the processing of data or when the controller or processor is a public authority, e.g. in hospitals.

4.4 Do the regulations define the scope of data use?

The GDPR and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data adopt a definition of "processing", which includes both the use and the sharing of personal data: "'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." (art. 4.2 GDPR and art. 5 and 26.2 Law on the Protection of Natural Persons with regard to the Processing of Personal Data).

4.5 What are the key contractual considerations?

Compliance with the GDPR and national implementing laws is required when the controller or processor of personal data is established in the EU, as well as when the processing of personal data concerns data subjects who are in the EU (if related to the offering of goods and services or the monitoring of behaviour of data subjects within the EU). The provider of a mobile health app will thus have to comply with the GDPR

© Published and reproduced with kind permission by Global Legal Group Ltd, London

when offering services in Belgium, even though neither the controller nor the processor of personal data is located within the EU. Additionally, whenever a processor processes data on behalf of a controller, a data processing agreement compliant with art. 28.3 GDPR is required. For instance, if a physician makes use of a medical device for the diagnosis or follow-up of her/his patients and personal data will be processed by the medical device provider, the physician is compelled to conclude a data processing agreement with the medical device provider.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

In order to assure confidence of a patient in the healthcare industry and protect an individual's data and privacy, adequate safeguards must be provided to ensure personal data is not shared with third parties without a patient's knowledge and without their consent. In an information society, the obligation to professional secrecy no longer suffices to protect a patient's medical data.

5.2 How do such considerations change depending on the nature of the entities involved?

See question 4.2 above. Data protection laws must ensure that the personal data collected by a physician, a medical device or a health app is, on the one hand, not shared with, for example, insurance companies but, on the other hand, can be consulted by a physician administering emergency care.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The sharing of data is considered to be another aspect of the processing of data under Belgian law. Correspondingly, the same regulatory requirements apply (see question 4.3 above). As for the "secondary use" of data, when processing data for a purpose other than that for which the personal data have been collected (which is not based on the data subject's consent), the controller must ascertain whether or not the new purpose is compatible with the purpose for which the personal data was initially collected (art. 6.4 GDPR).

6 Intellectual Property

6.1 What is the scope of patent protection?

Inventions, in all fields of technology, are patentable if they are new (in other words; they are not part of the state of the art), if they are the result of the inventiveness or resourcefulness of the inventor, and if they are capable of industrial application (Title 1 of Book XI of the Code of Economic Law and Part II of the European Patent Convention). Software and mathematical methods are specifically exempt from patent protection, however, only to the extent that a patent application relates solely to software or mathematical methods as such. One can apply for patent protection for "mixed inventions", for instance for a new product of a technical nature which incorporates a software program. The European Patent Office classifies AI and machine learning-related applications as mathematical methods in its guidance. Patents are valid for 20 years. No legal regulation governs the inventions of employees, hence, employer and employee may freely allocate ownership of the patent rights of inventions created in the performance of the employee's duties. Lastly, Belgium has ratified the European Unitary Patent Package, including the Unified Patent Court Agreement and is awaiting the entry into force of the latter.

6.2 What is the scope of copyright protection?

Copyright protects literary or artistic works in a broad sense (Title 5 of Book XI of the Code of Economic Law). The work must be expressed in a specific form and meet a requirement of originality (the work must contain elements which are an expression of the author's own intellectual creation). The author of a work that fulfils these conditions is granted copyright protection without any formality, up until 70 years after his death. Copyright includes both transferable property rights and inalienable moral rights. The expression of software is also protected by copyright, as well as databases which meet the requirement of originality.

6.3 What is the scope of trade secret protection?

Information is considered a trade secret if the information is secret, not publicly known or easily accessible, if the information has commercial value due to its confidentiality, and if the information was made subject to reasonable measures to protect its confidentiality (Title 8/1 of Book XI of the Code of Economic Law). Trade secrets are not protected by an intellectual property right but the wrongful acquisition of such information is prohibited and may be enforced in court by means of a claim for injunctive relief and damages. In addition, the malicious or deceptive disclosure of secrets of the factory in which someone has worked is criminally sanctionable (art. 309 Code of Criminal Law). Employees are also obliged to safeguard the trade secrets of their employers and any act of unfair competition is sanctionable (art. 17 of the Law concerning Employment Contracts of 3 July 1978 and art. VI.104 of the Code of Economic Law).

6.4 What are the typical results on academic technology transfer rules?

The intellectual property rights of creations by employees of academic institutions are normally transferred to the academic institution in exchange for an equitable share of the monetary proceeds from the exploitation of the invention. Universities in Belgium usually have their own technology transfer department. For instance, the KU Leuven Research and Development Tech Transfer Office is responsible for industry collaboration, IP management and the creation of spin-off companies at the Catholic University of Leuven, Europe's most innovative university. Universities generally aim to retain the intellectual property rights of their research results and grant exploitation licences to the industry.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

As said above, software may be protected by a patent if incorporated in technology, such as a medical device. In addition, the expression of software enjoys copyright protection if it is original in the sense that it is the author's own intellectual creation (Title 6 of Book XI of the Code of Economic Law). The

© Published and reproduced with kind permission by Global Legal Group Ltd, London

employer is considered to acquire the copyright property rights of software developed by employees either in the performance of their duties or on behalf of their employer.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The IP rights to collaborative improvements need to be carefully allocated when concluding agreements. In agreements between industry and healthcare, the transparency rules need to be complied with. As of 2018, industry associations voluntarily self-regulated and disclosed their interactions on www.betransparent.be. With the introduction of the Sunshine Act of 18 December 2016, all actors are now legally obliged to yearly disclose their interactions with healthcare professionals. Also, AI data platforms (e.g. Lynxcare) prove to be a valuable partner for hospitals and healthcare professionals providing insights to improve the quality of care and patient experience in Belgian hospitals; GDPR considerations may not, however, be neglected.

7.2 What considerations apply in agreements between health care and non-health care companies?

In any collaboration in the healthcare industry, one must be wary of anti-competitive agreements. The (health) tech and pharmaceutical landscape is often characterised by major players, so caution needs to be exerted when contracting. In addition, the healthcare industry is one of the highest regulated sectors. The healthcare company must take the lead in assuring that the non-healthcare company understands and abides by healthcare regulations whenever it applies to the latter.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning (ML) is valuable for a broad array of applications in digital health. Machine learning facilitates predictive and personalised healthcare and increases its efficiency. For example, ML can predict exacerbations based on physiological signals in patients suffering from chronic diseases. Personalised medicine is another one of its great advantages. Particularly in the healthcare sector, which is characterised by limited resources, machine learning is expected to improve the quality of patient care.

8.2 How is training data licensed?

Licensing training data is relatively new. The Database Directive laid some of the groundwork in facilitating the licence of vast amounts of data. Databases may be protected either through copyright protection, if the structure of the database is sufficiently original, or through the *Sui Generis* Database Right (SGDR) for the substantial investment in obtaining, verifying or presenting the content of the database (or through both) (Title 7 of Book XI of the Code of Economic Law). Under the SGDR, the extraction and reuse of substantial parts of a database can be commercialised for a period of 15 years from the creation date of the database or from the moment the database first became publicly available.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

According to the case law of the Court of Justice, copyright protection is merely possible if the author has been able to express his creative abilities by creating free and creative choices that give a personal touch to the work. A work, made or improved by ML, cannot be protected by copyright if it is created without creative human involvement and does not meet the requirement of originality. As with regards to patents, according to the European Patent Office, algorithms are *per se* of an abstract mathematical nature and normally exempt from patent protection. If not exempt from patentability, for example when incorporated in technology, other problems occur. When AI is merely used as a tool to aid a researcher in the development of an invention, the researcher shall still be the inventor. It becomes more complicated if human involvement is limited or non-existent. Problems may arise with the condition of inventiveness if the human intervention in the creation of an invention did not require any originality, creativity or intellectual contribution from the researcher. Under current (European) patent law, an inventor can only be a person and AI cannot be seen as the inventor. The question arises in such cases whether it is more adequate to allocate the patent to the developers of the AI technology or to the owners of the AI technology, rather than to the person who "notices" the invention developed by AI (the "researcher").

8.4 What commercial considerations apply to licensing data for use in machine learning?

The world's most valuable resource is said to be no longer oil but data. The quality of the data used in ML is essential for the quality of the results it presents. Therefore, companies developing AI technology will become increasingly interested in (exclusive) licences on quality datasets with the least restrictions possible. On the other hand, Belgian data protection regulation principally prohibits the processing of health-related data, unless an exception, such as consent of the data subject, applies. Moreover, the principle of data minimisation and the restrictions on data processing for a purpose other than for which it was initially collected, may directly clash with the commercial interests of tech companies.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Besides the general regimes of contractual and extra-contractual liability, the regimes of product liability and medical liability must be considered. Product liability is based on strict liability. A party claiming damages must only demonstrate a defect in the product, the damage and the causal relationship between the defect and the damage. The fault of the manufacturer need not be established. A product is defective if it does not provide the safety one is entitled to expect from that product. Any person in the production chain, the EU importer and the supplier may be held liable. As such, a physician or hospital may take the role of manufacturer or supplier of a defective product. Furthermore, a two-track system exists for medical liability in Belgium. On the one hand, the patient can invoke the medical liability of its

© Published and reproduced with kind permission by Global Legal Group Ltd, London

physician or the hospital. On the other hand, a fund has been established to compensate severe damage caused by "medical accidents without liability".

9.2 What cross-border considerations are there?

Within the EU, product liability is more or less harmonised and a patient suffering damages from a defective product such as a medical device will be granted similar protection in all member states. The EU importer can also be held liable in the same manner as a foreign manufacturer can be. However, as for medical liability, the Law on Medical Accidents of 31 March 2010, providing compensation for medical accidents without liability, only applies to healthcare provided on Belgian territory (regardless of the patient's nationality). Several other countries do not have a regime for faultless medical liability; accordingly, a Belgian patient may not enjoy equal protection when receiving healthcare services abroad. Lastly, the European Union Directive on the Application of Patients' Rights in Cross-Border Healthcare is taking its first steps in ensuring proper professional liability insurance in cross-border healthcare within the EU.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

First, whenever any personal data is transferred outside the EU/EEA, adequate measures need to be taken in order to ensure that the personal data is treated with equal protection to how it would be in the EU. The Commission has indicated certain countries as providing adequate protection but absent such a decision, personal data may only be transferred if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Even without transfer outside the EU/EEA, the GDPR shall have to be complied with when personal data is not anonymised. It also needs to be noted that any communication of personal data contained in electronic health records requires the authorisation of the Social Security and Health Chamber of the Information Security Committee.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Entering the healthcare industry means entering a highly regulated context, in which innovating might be challenging. Market strategies shall have to be adapted to the specific regulatory framework governing health products and services. For instance, the promotion of medical devices has been severely restricted. Further, the company shall have to be prepared to invest heavily in compliance, e.g. data protection laws, medical device regulation, product safety, etc. Lastly, the company will have to bear in mind that it will have to represent the interests, not only of the end-user, but also of doctors, hospitals, health insurance providers and the Belgian National Institute for Health and Disability insurance (NIHDI).

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

To assess the growth potential and the relative strength of a digital healthcare venture among its competitors, one needs to take account of certain elements. It is important to evaluate the IP protection the venture has obtained for its product, whether the product shall classify as a medical device or not and whether reimbursement has been obtained or is foreseeable to be obtained in the near future. This may require some contacts at the NIHDI, since reimbursement schemes are still in progress. The safety of the product and potential risks for liability claims need to be determined and one needs to ensure that there is a market for the health product, consisting not only of end-users, but also physicians and hospitals willing to prescribe or use the product in their provision of healthcare services.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Olivier Van Obberghen was trained as an M&A and commercial transactions lawyer. Since 2009, Olivier works exclusively for clients in the Life Sciences and Innovative Technologies sectors. He co-heads the Life Sciences department of Quinz together with Pieter Wyckmans.
Olivier's initial expertise in the Life Sciences sector was mainly transactional. His transactional expertise covers the entire life cycle of a drug product (R&D, clinical trials, supply chain and technical operations, commercial distribution), including M&A, product divestments and licensing deals (both early stage and established brands).
Since 2013, Olivier's practice has focused on healthcare compliance, tackling questions on the promotion of drug products and medical devices, on interactions with HCPs/HCOs, on patient support programmes (and patient involvement throughout a product life cycle), and on the use (and commercialisation) of healthcare data.
Olivier worked in-house for the legal department of UCB.

Quinz
Medialaan 28B
B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: olivier.vanobberghen@quinz.be
URL: www.quinz.be

Pieter Wyckmans provides expert advice to companies and organisations active in the (bio-) pharmaceutical, biotech and smart devices sectors. Pieter co-heads the Life Sciences department of Quinz together with Olivier Van Obberghen.
Pieter's transactional expertise covers the entire life cycle of a drug product (R&D, clinical trials, supply chain and technical operations, commercial distribution), including M&A, product divestments and licensing deals (both early stage and established brands).
Over the last few years, Pieter has developed a particular Life Sciences regulatory expertise under EU and national laws. More specifically, Pieter provides his clients with expert advice on a broad array of legal and strategic issues regarding clinical trials and market access, including early access programs, marketing authorisation procedures and pricing and reimbursement.
Pieter worked in-house for the legal department of UCB.

Quinz
Medialaan 28B
B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: pieter.wyckmans@quinz.be
URL: www.quinz.be

Amber Cockx is a corporate lawyer with a main focus on the Life Sciences sector. Amber has a background in intellectual property law and provides transactional and regulatory support to clients active in the pharmaceutical and medical devices sector. Her main areas of expertise comprise transactional and regulatory assistance throughout the entire product life cycle, from negotiating and drafting contracts, coordination of international R&D collaborations (H2020, IMI2), through clinical phases, marketing authorisations, advertising and promotion, pricing and reimbursement, and interactions with healthcare professionals and healthcare organisations.

Quinz
Medialaan 28B
B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: amber.cockx@quinz.be
URL: www.quinz.be

Quinz is a Brussels-based law firm with a strong focus on Life Sciences. Quinz assists the global, regional (EMEA, LATAM, APAC) and local (Belgian, Luxembourg and the Netherlands) legal departments of pharmaceutical companies on a broad array of (strategic, operational, licensing and M&A) transactions throughout the life cycle of a life sciences product. Quinz has also developed a sound expertise in regional and local regulatory work (including pricing and reimbursement, clinical trials, data transparency, marketing authorisation procedures, cGMP) and compliance matters (including transfers of value, promotion of life sciences products, antitrust compliance questions, patient directed programmes, GDPR).
Quinz was founded in 2011. Its Life Sciences department is headed by Pieter Wyckmans and Olivier Van Obberghen.
Clients include: Janssen Pharmaceutica; UCB; Takeda; Novo Nordisk; and Roche.

www.quinz.be

QUINZ | ADVOCATEN AVOCATS ATTORNEYS

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Brazil


Ana Karina E. de Souza


Diego de Lima Gualda


Elton Minasse


Carolina de Souza Tuon

Machado Meyer Advogados

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

"Digital health" is the use of technology in healthcare in order to make it more dynamic, efficient and agile and, consequently, increase the quality of services to be provided and patient safety.

Thus, "digital health" allows the use of information technologies to treat patients, conduct research, promote learning and training, and also monitor diseases.

Finally, "digital health" also allows the incorporation of machines, mobile devices and artificial intelligence to capture information and use them for the sake of medicine and patient well-being.

1.2 What are the key emerging technologies in this area?

In the Brazilian market, the key emerging technologies in digital health are as follows: (i) artificial intelligence; (ii) big data; (iii) automation; (iv) mobile applications; (v) wearables; and (vi) telemedicine.

Artificial intelligence is based on technology that simulates human reasoning, and it contributes to the improvement of clinical and hospital processes and assists in managing information at these locations. An example of use of artificial intelligence is automated attendance, which streamlines patient care and solves common questions quickly and easily.

Big data is the storage of a large volume of data that can be organised in the Cloud, which makes it easier for employees to work and optimise time.

Automation will allow more accurate diagnostics and more personalised treatments. In addition, the use of machines has offered considerable gains, such as greater accuracy, minimal cuts and reduced scar size in surgery.

Mobile applications and wearable devices can help increase chronic disease prevention, reduce risk factors and improve the quality and life expectancy of users.

Finally, telemedicine allows the use of technologies to remotely perform diagnostics, monitoring and care.

1.3 What are the core legal issues in health care IT?

The issues for digital health in Brazil are: (i) the difficulty to ensure the security and privacy of information that is shared by patients; (ii) computer integration of the Brazilian public health system; (iii) absence of a specific regulatory framework; (iv) various authorities regulating the sector; (v) changing behaviours and routines to adhere to new technologies; and (vi) lack of financial and technological resources.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The Brazilian Federal Constitution establishes, in article 196, that health is a right of the people and a duty of the State and shall be guaranteed by social and economic policies aimed at (i) reducing the risk of illnesses and other hazards, and (ii) the universal and equal access to actions and services for promotion, protection and recovery thereof.

Article 198 of the Brazilian Federal Constitution also provides that public health actions and public services integrate a regionalised and hierarchical network and constitute a single system, organised according to the following guidelines: (i) decentralisation, with a single management in each sphere of government; (ii) full service, priority being given to prevention actions, without prejudice to assistance services; and (iii) community participation.

In addition, access to health is a social right, guaranteed in article 6 of the Brazilian Federal Constitution, pursuant to the human dignity principle.

The Federal Council of Medicine ("CFM"), as established by Law 3,268, of 30 September 1957, has the task of overseeing professional ethics and, at the same time, judging and regulating the medical profession.

Law 12,842, of 10 July 2013, specifically provides for the practice of medicine and also confirms that new medical procedures and therapies for regular use in Brazil must necessarily be analysed by the Federal Council of Medicine regarding several aspects such as safety, efficiency, convenience and benefits to patients.

Those are the main legal statutes that regulate healthcare in Brazil.

2.2 What other regulatory schemes apply to digital health and health care IT?

In Brazil, healthcare IT regulation is still under development.

Among the main regulations that influence the relationship between technology and health, there are: (i) the Civil Framework of the Internet ("*Marco Civil da Internet*", in Portuguese) and its respective regulating decree; (ii) the Access to Information Law ("*Lei de Acesso à Informação*", in Portuguese); (iii) the General Data

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Protection Law ("*Lei Geral de Proteção de Dados*", in Portuguese); (iv) the National Policy for Technological Innovation in Health ("*Política Nacional de Inovação Tecnológica na Saúde*", in Portuguese); (v) the Electronic Health Record Law ("*Lei do Prontuário Eletrônico*", in Portuguese); (vi) the Resolutions of the Federal Council of Medicine; (vii) the Medical Code of Ethics; and (viii) the resolutions of the National Supplementary Health Agency ("ANS") and National Health Surveillance Agency ("Anvisa").

The Marco Civil da Internet (Law No. 12,965/2014) and its regulating decree (Decree No. 8,771/2016) set forth the guidelines for internet use in Brazil, indicating procedures for data storage and protection to be observed by connection and application providers.

The Access to Information Law (Law No. 12,527/2011) establishes guidelines for the Federal Government, States, Federal District and Municipalities to provide the people with access to information.

The General Data Protection Law (Law No. 13,709/2018) protects sensitive personal data, including relating to health.

The National Policy for Technological Innovation in Health (Decree No. 9,245/2017) regulates hiring and acquisitions that involve strategic products and services for the Brazilian public healthcare system (*Sistema Único de Saúde*, ("SUS")).

The Electronic Health Record Law (Law No. 13,787/2018) provides for the digitalisation and use of computerised systems for storage and handling of patient records.

The Medical Code of Ethics (CFM Resolution No. 2,217/2018) establishes the rules and guidelines for medical practice (including education, research and administration of health services).

The Federal Council of Medicine, through Resolution CFM No. 1,643/2002, defines telemedicine as the practice of medicine through the use of interactive methodologies of audiovisual communication and data, aimed at healthcare, education and research. This Resolution requires that the appropriate technology be used in compliance with CFM technical standards regarding data safekeeping, handling, transmission, confidentiality, privacy and the guarantee of professional secrecy.

CFM Resolution No. 2,107/2014 regulates teleradiology, which consists in the practice of medicine, using information and communication technologies to send radiological data and images for the purpose of reporting, as support for locally developed activities.

Resolution CFM No. 2,264/2019 regulates telepathology, which consists in the exercise of medical specialty in pathology upon mediation by technologies for sending data and images for the purpose of reporting, in support of anatomopathological activities developed locally.

Within the specific scope of SUS, Resolution CIT No. 6/13, of the Ministry of Health, rules are set forth for the implementation of new applications, health information systems or new versions of existing systems and applications involving SUS and which are used by the Ministry of Health and the State, Federal and Municipal Health Departments.

In addition, digital health is the object of CIT Resolution No. 19 of 22 June 2017, which established the strategy for incorporating digital health into SUS, being named "digi-SUS".

With "digi-SUS", the Ministry of Health intends to guide, at national level, the various initiatives in this area currently developed in an unintegrated manner. A central element to this strategy being developed in Brazil is the implementation of electronic medical records, which is being carried out through the Programa de Informatização das Unidades Básicas de Saúde ("PIUBS").

Through the program, the Ministry has accredited companies to develop, make available, maintain and train health professionals in the use of hardware and software for the implementation of electronic medical records. However, the vast majority of units do not yet have an electronic medical record system.

In addition, Decree No. 9,795 of 17 May 2019, of the Ministry of Health, establishes guidelines for telehealth in Brazil within SUS.

Thus, as stated above, Brazilian regulation on digital health is still under development, there being no specific regulatory framework in relation thereto.

2.3 What regulatory schemes apply to consumer devices in particular?

"Mhealth" is medical and public health practice supported by mobile devices such as smartphones, patient monitoring devices, personal digital assistants and other wireless devices.

In Brazil, Resolution CIT No. 6/13, of the Ministry of Health, establishes rules for the implementation of new applications, health information systems or new versions of systems and applications already existing within SUS and which are used by the Ministry of Health and Federal, State and Municipal Health Departments.

Thus, this Resolution applies specifically to consumer devices within the scope of SUS. As for consumer devices in general, there is no specific regulatory framework yet.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

Regarding regulatory authorities, the following stand out: (i) the Ministry of Health; (ii) the National Supplementary Health Agency; (iii) the National Health Surveillance Agency; and (iv) the Federal Council of Medicine.

The Ministry of Health has the task of setting forth conditions for the promotion, protection and recovery of the health of the Brazilian population, reducing diseases, controlling endemic and parasitic diseases, and improving health surveillance, thus providing a better quality of life to the population.

The National Supplementary Health Agency ("ANS") is the regulatory agency linked to the Ministry of Health responsible for the health insurance sector in Brazil. Its task is to promote the defence of public interest in supplementary health care, regulate sector operators – including their relations with service providers and consumers – and contribute to the development of health actions in the country.

The National Health Surveillance Agency ("Anvisa") is a regulatory agency linked to the Ministry of Health, whose primary function is to promote the health of the population, acting in the sanitary control of various products, such as medicines, food and cosmetics, services and even the surveillance of ports, borders and airports.

Finally, the Federal Council of Medicine aims overseeing professional ethics throughout the country and, at the same time, judging and regulating the medical profession through regulatory action.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

In Brazil, although digital health regulation is still under development, some sensitive aspects of our legislation must be observed, even if there is no specific regulation. Thus, the areas of enforcement are: consumer rights; intellectual property; and data protection.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

The applicable regulation for Software as a Medical Device and its approval for clinical use is provided for under Anvisa's Collegiate Board Resolution ("RDC") No. 185, of 22 October 2001, which deals with registration, modification, revalidation and cancellation of medical products before Anvisa.

Medical equipment includes software such as medical devices (referred to as software), which is software that by itself (not including hardware) may be framed as a health product.

Although software is considered a medical device and subject to Anvisa regulation (RDC 185/2001 and RDC 40/2015), several rules do not apply to software, so, the creation of a specific regulation for software is currently under discussion by Anvisa.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

Overall, legal and regulatory concerns on the convergence of technologies with healthcare and medicine practices are related to the extension of digital health technologies' safety and efficiency, as well as how to address liabilities arising from new products as well as the associated professional practices. On the other hand, it is valid to highlight the revamped concerns around health information, particularly with respect to confidentiality, data privacy and information security. As the digital health technologies grow exponentially, authorities are also challenged to adapt the existing procedures to review, assess risks and approve the use of those new technologies.

Still, digital health technologies are very scarcely regulated in Brazil. On several fronts, regulators are gathering information and looking for international benchmarks, as well as conducting broader debates with civil society on proposing initial regulation. Meanwhile, for the technology that is already being applied, the cases will be ruled according to existing legislation particular to consumers, internet and data protection as well as broad principles of the law.

It is worth highlighting that even certain technological applications, broadly considered, remain unregulated in Brazil. Issues such as AI, Machine Learning, IoT are all in the process of political discussion with respect to the regulatory approach to be adopted. There are fundamental debates about the extent of human supervision, economic impacts in the labour market, algorithm bias, and discriminatory, among other issues. Without prejudice, with the recently enacted Brazilian Data Protection Law, Federal Law no. 13,709/2018 ("LGPD"), some of the concerns, as for example, automated process decision making, and discriminatory risks associated with such technology, are starting to have some specific legal treatment in Brazilian legislation.

- **Telehealth**

  Although regulatory debate on telehealth in Brazil is not new, there is no comprehensive regulation providing standards to its application which remains as a barrier to the expansion of telehealth in Brazil in scale. Telehealth is not forbidden and there are specific provisions in the regulation of the Medical Federal Council ("CFM"), as well as medical state councils, providing opinions and punctual standards for the practice. In February 2019, CFM made an attempt to consolidate several sparse regulations/opinions on telehealth, as well as to provide general standards for its practice, through Resolution no. 2.227/18 of the CFM. However, after the initial reaction of the medical professional community, the CFM has decided to revoke the Resolution and to continue the debate.

  Main regulation issues

  Liability for negligence/malpractice (improper application of telehealth technology): In article 37, the Medical Code of Ethics (issued by CFM) prohibits that practitioners prescribe treatment or other procedures without a direct examination of the patients. However, it does foresee that telehealth for distance medical care will be regulated specifically by the CFM. In article 4, Resolution no. 1.643/2002 of the CFM makes it clear that the professional responsibility for distance care lies with the attending physician of the patient, and others involved (such as the manufacturer of the digital appliances) will respond jointly and severally in proportion to the damage they have directly caused. Resolution no. 2.227/18 has proposed that only in exceptional situations would the telehealth be allowed without an in-person first examination.

  Unconsented sharing of sensitive data/use of data for purposes: The LGPD defines ethnicity, gender and health related personal data as sensitive personal data. Sensitive personal data is a special category of personal data which brings a more pervasive risk to negatively affect data subjects' human rights, which is the reason why the LGPD has limited the legal basis by which such personal data can be processed as well as increased the level of responsibility of data controllers (according to the LGPD: natural person or legal entity, of public or private law, that has competence to make the decisions regarding the processing of personal data). An important consideration of the regulation of telehealth is how to address aspects related to consent and data sharing, provided that such regulation will need to be aligned with the general data protection principles and discipline of the LGPD.

  Security of information of telecommunications/confidentiality: There are concerns over the quality of telecommunication infrastructure in Brazil, especially, to what extent limitation of such infrastructure would negatively affect the support to patients in the context of telehealth. By the same token, issues connected to information security and data breaches are also a source of concern. The LGPD now requires that data controllers must adopt security measures in order to mitigate risks of data breach, however there is no specific regulation of information security standards for the health sector. In the case of data breaches/security incidents, potential liabilities may arise from administrative/criminal/civil perspectives if proven that there were not proper measures in place/data controllers failed to comply with the LGPD provisions in this regard. The LGPD liabilities are independent of other liabilities that may arise in connection to the specific legislation.

- **Robotics**

  There is no comprehensive regulation in Brazil with respect to the application of robotics in medical procedures, although robotics in medical surgeries is already a reality and it is in practice. The absence of proper regulation gives cause to legal uncertainty, especially on cases related to product liability and/or professional malpractice.

  Current regulation issues

  Absence of clear standards for professional requirements, training and certification for the operation of robotics: As there are no specific requirements, typically, health professionals are certified by the manufacturer of the equipment. There is no major oversight with respect to professionals' expertise and capabilities on the use of robotics.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Liability for negligence/malpractice: As outlined in the case of telehealth, for robotics there is also a significant concern on how to address cases of malpractice. For robotic surgeries, there is a specific challenge to regulate product and professional liabilities, and how such liability will be shared among the manufacturer, the surgeon and other professionals involved in the procedure.

- **Wearables; Virtual Assistants (e.g. Alexa); Mobile Apps; Software-as-a Medical Device; AI-as-a-Service; IoT and Connected Devices; and Natural Language Processing**

General provisions of the Consumer Defence Code apply with respect to product liabilities. Where the product or service involves an internet-based application component, Federal Law no. 12.965/2014, as regulated, the "Civil Framework of the Internet" which sets forth the legal framework for internet application providers, including internet users' rights with respect to such providers, will also be applicable. Finally, with respect to personal data processing, the recently enacted Brazilian Data Protection Law will apply.

Main regulation issues

Product and service liability: The Consumer Defence Code set forth strict liability in connection to malfunctioning and defects of products and services. It also establishes the obligation to providers to be accurate and provide transparent information about the conditions of the use and safety specifications. Although eventual features or technological limitations are not considered a defect, providers will need to pay attention to product capability claims, not only to avoid misleading communication, which is considered illegal, but also to not attract further liabilities based on promises made by the product or service description. Except where approved and when reliable, providers shall be extremely careful with claims related to capabilities to monitoring or providing diagnoses of health conditions. Furthermore, in the absence of provisions regulating liabilities arising out from the use of new technologies, such as AI and Machine Learning, providers will assume all risks connected to the use of such technology in association to products' and services' commercial claims. The Civil Framework of Internet provides additional contractual and legal assurances, particularly with respect to freedom of communication, information and privacy, whenever an internet component (an application, website, platform) is associated with the product and/or service.

Personal data processing, sensitive personal data and data sharing: Considering the processing of personal health information, providers offering the solutions above will be under intensive scrutiny with respect to privacy, data protection practices and information security. The LGPD defines heath information that is related to an individual as sensitive personal data, which brings higher standards for data controllers (those providers) with respect to the processing of user information in connection to those products and/or services. Besides the requirement of observing the LGPD data protection principles, including data minimisation, prevention of security incidents and accountability, providers will need to make sure that personal data is processed in accordance with the legal basis set forth by LGPD, especially for sensitive personal data. Specific and separated consent may be required, and legitimate interest will not be available for personal data processing of health-related information. Furthermore, it will be important to pay attention to information security standards in order to prevent, as possible security incidents, compromising the related personal data; and, in the eventuality of an incident, to be ready to immediately respond and remediate damages. Liabilities in connection to the violation of LGPD are substantial and the fines applicable by the National Data Protection Authority ("ANPD") can go as high as R$ 50,000,000.00. Finally, it will be important to pay attention to personal data sharing. Considering the risks involved with personal sensitive data, including potential discriminatory use, the provider shall be particularly careful with personal data sharing with other controllers. As a rule, LGPD forbids sharing health information of a data subject in order to obtain economic advantage.

3.2 What are the key issues for digital platform providers?

Digital platform providers shall be concerned with the extension of its liabilities in light of the nature of the product or service offered. As provided above, existing legislation in Brazil, applicable to consumer defence, internet users and personal data subjects, is already comprehensive in terms of the rights that individuals are entitled to when contracting with digital platforms. It is expected that new technologies (AI, Machine Learning, IoT, etc.) will add more complexity to the debate related to digital platform providers. Product and service liabilities, product and service permits (and approval process), privacy, data protection and information security are the main themes digital platform providers shall pay attention to in Brazil. It is also expected that health authorities provide further specific regulation in the context of the consolidation of technologies aiming to offer digital health products and/or services.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Regarding data protection legislation, the main applicable laws in Brazil are the Internet Civil Framework, that establishes the guidelines for internet use in Brazil, the LGPD and the Brazilian Consumer Defence Code. There is also specific legislation applicable to the protection of medical and health information confidentiality and handling.

The LGPD was enacted in 2018 and set forth the general regulation of personal data processing in Brazil. It was highly inspired by the provisions of the European General Data Protection Regulation (GDPR) and, like the GDPR, is demanding many financial and human resources from organisations that need to adapt to the new LGPD standards.

The LGPD will become effective in August 2020 and the most important features of the law are: (i) the guarantee of extensive rights to data subjects (access, rectification, anonymisation, portability, elimination, and opposition, among others); (ii) a set of principles that organisations are required to observe when processing personal data, highlighting a principle of data minimisation and accountability (demonstration of compliance); (iii) information security requirements; and (iv) significant liabilities to organisations that violate the law (including the application of penalties as high as R$ 50,000,000.00 per violation).

It is important to highlight that health information that is related to an individual is considered to be sensitive personal data under the LGPD. Given the increased risks that the processing of sensitive personal data may present to data subjects, sensitive personal data can only be processed based on exceptional legal

© Published and reproduced with kind permission by Global Legal Group Ltd, London

bases. Particularly, sensitive personal data processing may be subject to specific and separated consent and legitimate interest is not available to justify its processing. With respect to health information, the LGPD set forth that, as a rule, such information shall not be processed to obtain economic advantages. Liabilities connected to violation of the LGPD with respect to sensitive personal data will be higher.

4.2 How do such considerations change depending on the nature of the entities involved?

The provisions of the LGPD are applicable to any personal data processing carried out by a natural person or a public or private entity. Therefore, as a rule, the nature of the entity will not change the considerations above with respect to the LGPD. There are some exceptions with respect to the purpose of the data processing (e.g. for journalism, academic purposes or public safety) and there is a specific legal basis (or regulation) for the personal data processing for certain entities, as research entities, health service providers, or the entities of the public administration. That being said, the core aspects of the law, in particular the obligations that personal data processing agents need to comply with, will be applicable regardless of the nature of the entity involved.

4.3 Which key regulatory requirements apply?

Personal data processing shall be performed in accordance to the following principles: purpose; adequacy; need; free access; quality; transparency; security; prevention; non-discrimination and accountability. It must be processed in accordance with a valid legal base (consent, legal obligation, research for research entities only, execution of contract, protection of life and physical integrity, heath tutelage in procedure performed by health professionals/services/authorities and legitimate interest). When processing sensitive personal data or for international data transfer, specific requirements as set forth by the law will apply. Data controllers shall keep an updated registry about all personal data processing. It is also important to comply with data subject rights (access, rectification, anonymisation, portability, opposition, etc.), as well as to adopt organisation and technical measures to protect personal data against unauthorised access or use. Organisations shall be able to demonstrate compliance with the provisions of the law.

4.4 Do the regulations define the scope of data use?

Yes, especially in regard to the informed purposes for data processing. As mentioned above, processing must be limited solely and exclusively to the data required to achieve a defined purpose, in accordance with the legal basis applicable and data subjects shall be able to access and understand the purpose of the processing. Exclusion/deletion of unused data must be carried out frequently and as soon as possible, and channels for communication with the data subjects must be made available to exercise data subject's rights.

4.5 What are the key contractual considerations?

Specifically, when negotiating with business partners or providers, organisations shall assess to what extent such partners or providers will process personal data that is being provided by that organisation, as well as in what capacity they will process such personal data – as controllers or processors. Data controllers shall make sure that data processors are able to comply with the data protection legislation as they may be jointly and severally liable for the data processors' violation of the law. Data controllers shall also include in the agreements all the instructions about the standards applicable to the data processing that shall be carried out by the data processor.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The key issue to be considered is to make sure there is an appropriate legal base for data sharing. In many instances, it may be required to obtain data subject specific and separated consent for data sharing with a different data controller. Another key consideration is to observe the existing restriction set forth by the LGPD with respect to the communication and sharing of health information related to an individual with the aim to obtain economic advantage. It is also important to properly address liability concerns as the joint controller situation may attract liability to the original data controller.

5.2 How do such considerations change depending on the nature of the entities involved?

Again, the existing nuances in the LGPD will not materially change the obligations that entities of different natures will have with respect to the core aspects of the LGPD. Typically, with respect to data sharing, the LGPD provides stricter regulation with respect of certain kinds of entities. For example, article 13 of the LGPD determines that entities conducting public health studies may have access to personal databases, which shall be processed exclusively within the entity and strictly for the purpose of carrying out studies and research and shall be kept in a controlled and secure environment, in accordance with security practices provided in specific regulation and that include, whenever possible, anonymisation or pseudonymisation of the data, as well as taking into account the proper ethical standards related to studies and research. In addition, such entities are prevented from sharing this information with third parties.

5.3 Which key regulatory requirements apply when it comes to sharing data?

As provided above, the key regulatory requirement is the evaluation of a valid legal base authorising data sharing, as well as legal purpose. For sensitive personal data and international data transfer, additional requirements may apply.

6 Intellectual Property

6.1 What is the scope of patent protection?

The main applicable law in Brazil for patent protection is the Industrial Property Law (or Federal Law no. 9,279/1996) that establishes the rights and obligations related to industrial property. Industrial property is the section of intellectual property that addresses intellectual creations related to industry, trade and services provision and protects inventions, industrial drawings, trademarks and geographical indications.

The guidelines for Brazilian Patent Protection are the following:

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- **Types of Patents**: the Industrial Property Law contemplates two types of patents:
  - **Invention patent**: any invention that fulfills the requirements of novelty, inventive activity and industrial application is patentable.
  - **Utility model patent**: any object of practical use, or part thereof, that is susceptible of industrial application, presents new shape or arrangement and involves an inventive act that causes a functional improvement in its use or manufacture, is patentable.
- **Inventor of invention or utility model**: has the right to obtain the patent that grants the ownership of the invention or the utility model.
- **First-to-file rule**: the Industrial Property Law provides that the right to obtain the patent will be granted to the inventor who first filed the patent request, independently of the dates of invention or creation.
- The following are not considered inventions or utility models:
  - discoveries, scientific theories and mathematical methods;
  - purely abstract concepts;
  - schemes, plans, principles or methods of a commercial, accounting, financial, educational, publishing, lottery or fiscal nature;
  - literary, architectural, artistic and scientific works or any aesthetic creation;
  - computer programs *per se*;
  - the presentation of information;
  - rules of games;
  - operating or surgical techniques and therapeutic or diagnostic methods, for use on human or animal bodies; and
  - natural living beings, in whole or in part, and biological material, including the genome or germ plasm of any natural living being, when found in nature or isolated therefrom, and natural biological processes.
- **Novelty**: inventions and utility models are considered new when not included in the state of the art, which comprises everything made accessible to the public before the date of filing of a patent application, by written or oral description, by use or any other means, in Brazil or abroad. To determine novelty, the content of a filed application in Brazil, but not yet published, will be considered as state of the art from the filing date or from the priority claimed, and is considered to be published, even though publication happens subsequently. Such provisions apply to an international patent application filed in accordance with a treaty or convention in force in Brazil, provided that there is national processing. The disclosure of an invention or utility model which occurs during the 12 months preceding the date of filing or priority of the patent application will not prejudice the novelty, provided such disclosure is made by:
  - the inventor;
  - the INPI (National Institute of Industrial Property), by means of the official publication of a patent application filed without the consent of the inventor and based on information obtained from him or as a result of his acts; or
  - third parties, based on information directly or indirectly received from the inventor or as result of his acts.
- **Inventive activity**: when a person is skilled in the art:
  - an invention does not derive in an evident or obvious manner from the state of the art; and
  - a utility model does not derive in a common or usual manner from the state of the art.
- **Industrial application**: inventions and utility models are considered susceptible of industrial application when they can be made or used in any kind of industry.
- **Patent grant**: a patent will be granted after the application is allowed and, after the payment's proof of the corresponding fee, the respective letters-patent will be issued. The patent will be considered granted as of the date of publication of the respective act.
- **Patent protection term**:
  - invention: 20 years, counted as from the filing date; and
  - utility model: 15 years, counted as from the filing date.
- **Protection conferred by a patent**: extension of patent protection will be determined by the content of the claims, interpreted accordingly to the specification and drawings. A patent grants its owner the right to prevent third parties from manufacturing, using, offering for sale, selling or importing for such purposes, without his consent:
  - a product that is the subject of a patent; and/or
  - a process, or product directly obtained by a patented process.
- The protection does not apply:
  - to acts executed by unauthorised third parties privately and without commercial scope, provided they do not prejudice the patentee's economic interests;
  - to acts executed by unauthorised third parties for experimental purposes, related to studies, scientific or technological research;
  - to the preparation of a medicine according to a medical prescription for individual cases, executed by a qualified professional, as well as to a medicine thus prepared;
  - to a product manufactured in accordance with a process or product patent that has been placed on the internal market directly by the patentee or with his consent;
  - to third parties who, in the case of patents related to living matter, use the patented product without economic ends as the initial source of variation or propagation for obtaining other products; and
  - to third parties who, in the case of patents related to living matter, use, place in circulation or commercialise a patented product that has been introduced lawfully onto the market by the patentee or his licensee, provided that the patented product is not used for commercial multiplication or propagation of the living matter in question.
- **Patentee's rights**: a patentee has the right to obtain compensation for the unauthorised exploitation of the patent's subject matter, including exploitation that occurred between the date of the application's publication and that of the patent's grant.

6.2 What is the scope of copyright protection?

The main applicable law for copyright protection in Brazil is the Copyright Law (or Federal Law no. 9,610/1998) that establishes the rights and obligations related to copyright and related rights.

The guidelines for Brazilian Copyright Protection are the following:

- **Protection**: copyright protection is automatic upon the work's creation and there is no need of copyright registration to enforce such rights against third parties. All

© Published and reproduced with kind permission by Global Legal Group Ltd, London

acts that violate copyrights (moral and patrimonial) may be stopped by the author (such as reproduction, disclosure, adaptation, translation, and distribution). Moral copyright is a part of the author's personality right and, therefore, is not assignable, licensable and waivable. Patrimonial copyright is related to the economic exploitation that may be executed by the author in relation to its works and, therefore, the author may assign or license such patrimonial copyright.

- **Legal conditions**: all creations from a person expressed by any means, or affixed in any type of medium, tangible or intangible, are protected as intellectual work. Therefore, the main legal conditions for protection are: (i) the originality of the work; and (ii) the externalisation of the work in some form. That is, a simple idea is not protected by copyright.
- **Examples of works protected by copyrights**:
  - literary, artistic or scientific works;
  - lectures, speeches and other works of such nature;
  - dramatic works with or without music;
  - choreographic works and pantomimes, if the performance may by fixed in any form;
  - musical compositions, with or without words;
  - audio-visual works, with or without sound;
  - photographic works and related;
  - drawings, paintings, sculptures, geographical maps, plans, sketches and related;
  - adaptations, translations and other transformations of original works;
  - collections or compilations, databases and other works in which the selection, organisation or arrangement of their contents constitute intellectual creations; and
  - software (which is subject to specific regulation: Software Law – Law no. 9,609/1998).
- **Examples of works not protected by copyright**:
  - ideas, systems, methods, projects;
  - schemes, plans or rules to execute mental acts, games or businesses;
  - blank forms to be completed with any kind of information, scientific or not, and their instructions;
  - texts of laws, decrees, court decisions and other official acts;
  - information of common use, such as calendars, agendas, and captions;
  - isolated names and titles; and
  - industrial or commercial use of ideas within the works.
- **Term**: moral rights are perpetual and patrimonial copyright lasts 70 years as counted from 1 January of the year following the author's death (in the event of jointly owned works, such period will be counted from the death of the last co-author).
- **Ownership**: the owner of the work is its author. The commission agreement should provide ownership of the commissioned work. The labour agreement should provide ownership of work created by the employee. Regarding software, please see below.
- **Assignment and licence**: need to be executed in writing. Moral copyright is not assignable or licensable.
- **Indemnification**: in the event of copyright infringement, the damages will at least correspond to the profits and revenues arising out of the infringement. If those profits and revenues cannot be determined, the damages will be estimated considering the royalties that the copyright owner would have received if he had licensed such copyright.

In Brazil, software is also considered copyright, but the Software Law provides specific regulations that differ on some levels to the Copyright Law. The Software Law guidelines are the following:

- **Software definition**: software is the expression of an organised set of instructions in natural code language, contained in a physical support of any kind, necessarily employed in automatic machines for the manipulation of data, devices, tools or peripheral equipment, based on digital or analog technique, so they will operate in a determined way and with determined purposes.
- **Protection**: moral copyright does not apply to software, excepting the author's right to claim the software's authorship and to oppose any unauthorised changes when these result in the disfigurement, mutilation or any other modification to the software that harms the author's honour or reputation.
- **Term**: the rights related to the software are protected for a period of 50 years as counted from 1 January of the year following its registered publication or, when such register is unavailable, its creation. In the same way as copyright, a register is not necessary to grant the software's protection, as long as the legal conditions are met.
- **Ownership**: unless covenanted otherwise, the employer, commissioner or public body shall have full ownership of the rights of a software developed and elaborated throughout the duration of an agreement or legal obligation, expressly intended for research and development, or in which the employee's, commissioner's or server's activities are provided, or yet, which arise from the nature of the duties pertaining said relationships. Unless provided otherwise, the remuneration for the work or service provided shall be limited to the agreed remuneration or salary.
  - When the employee or commissioned services provider or server create a software with no connection to the employment agreement, commission agreement or legal obligation and without use of resources, technological information, trade and business secrets, materials, facilities or equipment of the employer, the company or entity which the employer, commissioner or public body has entered into a services agreement or similar agreements with, the employee, the commissioned services provider or server will have full ownership of the software's rights.
  - The provisions mentioned above are also applicable to grant-funded researchers and interns.
- **Derivations**: the rights over the derivations authorised by the owner of the software's rights, including their economic exploitation, will belong to the authorised person who affects them, unless otherwise provided.
- **Licence**: the use of a software in Brazil shall be the object of a licensing agreement:
  - All acts and agreements for the licensing of commercialisation rights relating to foreign software shall establish, regarding the payable taxes and charges, the liability for the respective payments and provide the remuneration for the owner of the software's rights, residing or domiciled abroad.
  - The following clauses shall be null and void: i) clauses limiting production, distribution or commercialisation, breaching applicable regulatory provisions; and ii) clauses exempting any of the agreement's parties for the liability for any third parties' lawsuits arising from misuse, flaws or violation of copyright.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

6.3 What is the scope of trade secret protection?

Trade secrets protection is mainly provided by the Industrial Property Law, which protects competitive relations in Brazil, one of its objectives being the repression of unfair competition. Other statutes grant the right of privacy, as well as the Brazilian Constitution.

However, the main provisions regarding trade secrets are in the Industrial Property Law:

- **Crimes of unfair competition**: a crime of unfair competition is committed by he or she who (including the employer, partner or administrator of the company):
  - discloses, exploits or uses, without authorisation, confidential knowledge, information or data, usable in industry, commerce or services provision, excepting that which is of public knowledge or which is obvious to a person skilled in the art, to which he has had access by means of a contractual or employment relationship, even after the agreement's end; and
  - discloses, exploits or uses, without authorisation, knowledge or information as mentioned in the previous item, when obtained directly or indirectly by illicit means or to which he has had access by fraud.
- **Penalties**: detention of three months to one year, or a fine.
- **Indemnification**: independently of the criminal action, the injured party may file civil actions that they consider suitable compensation that will be determined by the benefits that the injured party would have gained had the violation not occurred.
- **Further indemnification**: the injured party has the right to receive indemnification compensating the losses and damages caused by the acts of industrial property rights violation and unfair competition that are not provided in the Industrial Property Law, but tend to prejudice another's reputation or business, or cause confusion between commercial or industrial establishments or service providers, or between products and services placed on the market. In such cases:
  - the judge may, to avoid irreparable damages or damages that would be difficult to recover from, grant an injunctive order to suspend the violation; and/or
  - loss of profits will be determined by the following criteria which is the most favorable to the injured party: i) the benefits that the injured party would have gained if the violation had not occurred; ii) the benefits gained by the author of the rights' violation; or iii) the remuneration that the author of the violation has paid to the owner of the violated rights for a granted license which would have legally permitted him to exploit the rights.

6.4 What are the typical results on academic technology transfer rules?

In Brazil, the main law regarding technological and scientific research is Law no. 10,973/2004 (Innovation Law), which suffered an amendment by Law no. 13,243/2016.

The Innovation Law provides that the Brazilian Federal Government, States, Cities and their authorised entities may, according to specific regulations of each one of these, invest in companies that develop products or disruptive processes in accordance with the guidelines and priorities provided in the science, technology, innovation and industrial development policies of each sphere of government. Such investment will be executed by the acquisition of minority shareholding of those companies.

The intellectual property of such results will belong to the companies, unless otherwise provided in the relevant agreements. If the resulting intellectual property is licensed or assigned to the public entities abovementioned, they will need to use such resulting intellectual property in the general public interest.

ICTs (Scientifics, Technological or Innovative Institutions – "Technology Incubators") are public agencies or non-profit companies established according to Brazilian laws and headquartered in Brazil that deal in scientific research or new products, services or processes development. Public ICTs may execute technology transfer or licensing agreements related to the intellectual property developed solely by the Public ICT or by means of a joint effort with a company, including a Private ICT.

If the Public ICT is hired with an exclusivity obligation, the Public ICT offer must be published in its official website. If the Public ICT is in a joint effort with a company, this company may be hired with an exclusivity obligation. When the resulting intellectual property is assigned or licensed exclusively to the assignee or licensee, the technology transfer or licensing agreements may be directly executed, as long as they are related to exploitation or development scopes provided in specific regulation. The exclusive assignee or licensee will lose the right to exploit the resulting intellectual property if such intellectual property is not commercialised according to the terms and conditions provided in the agreement. In such an event, the ICT will be able to execute a new licensing. If the technology transfer or licensing agreements are executed, officers, inventors, servers, employees or service providers are obliged to provide the knowledge and information necessary to fulfil the agreement. If a Private ICT is remunerated for such technology transfer or licensing, its non-profit status will not be treated with prejudice.

The ICTs may execute joint effort agreements with public and private institutions to carry out scientific and technologic research, as well as technology, product, or service or process development. Those agreements must specifically provide on the ownership of the resulting intellectual property, as well as the shares on the results of such intellectual property exploitation. The ICT may assign all the intellectual property rights to the other party, as long as the other party provides financial compensation to the ICT, or non-financial compensation that must be economically measurable.

If provided specifically in the ICT regulation, the ICT may assign its resulting intellectual property rights to the inventor without charges, or to third parties, with charges. Such assignment must be expressly justified and provided by the ICT's highest authority and the technologic development area must be previously heard.

The Innovation Law grants to the author or inventor of the assigned or licensed intellectual property the following shares regarding the economic benefits of ICTs arising out of the assigned or licensed intellectual property:

- minimum of 5%; and
- maximum of ⅓.

Economic benefits shall mean any royalty, remuneration or financial benefit arising out of the intellectual property exploration.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

All software in Brazil (including software as a medical device) is protected in the same way as other kinds of software in Brazil. There are no specific intellectual property laws that would apply

© Published and reproduced with kind permission by Global Legal Group Ltd, London

to such type of software. If the software is part of a medical device involving other components (such as any hardware), the medical device may be protected by patent. The software itself would not in principle be subject to patent protection.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Controller and Processor apply to collaborative improvements.

7.2 What considerations apply in agreements between health care and non- health care companies?

Companies that provide healthcare services when contracting companies that supply digital platforms must establish agreements related to liability issues applicable to confidentiality, data privacy and information security.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Thus far, there is no regulation yet in Brazil regarding machine learning in digital health.

8.2 How is training data licensed?

Assuming that training data is personal data, a licence is not applicable, but only authorisation from the data subject regarding the use of their personal data for the training scope, is required. The LGPD shall apply to this hypothesis.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

In Brazil, the software's source code is protected by copyright, but not the algorithm itself. Therefore, improvements to algorithms resulting from machine learning are not protected by intellectual property rights in Brazil.

8.4 What commercial considerations apply to licensing data for use in machine learning?

In case the data used in the machine learning process corresponds to personal data, note that individuals (data subjects) would have to consent to such use, including if the company collecting the data intends to profit with such data by transferring it. In case the proper legal base for such processing activity has not been observed, the company can be subject to the consequences mentioned above in section 3 above. There is no specific licensing or regulatory procedure applied before data is used for the purpose of machine learning. Provided that the data protection issues indicated above have been observed, we note that data can be transferred for a commercial purpose since it constitutes an immaterial property of the company. However, a licensing agreement would apply only to items protected by the Brazilian Federal Law no. 9,610/98, the "Brazilian Copyrights Law". The Brazilian Copyrights Law does not protect data by itself but guarantees protection of databases. However, in order for such database to be protected, it must be organised in a creative or unique manner, so that it constitutes an intellectual creation. Although it is unlikely that the database used in machine learning will be considered an intellectual creation (and, therefore, subject to licensing), data constitutes an immaterial property of the company and its use and transfer can be the object of a commercial agreement under Brazilian law.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

On top of the liabilities arising from data protection issues, including penalties regarding violation of data subjects' rights and the principles set forth in the LGPD (subject to administrative, civil or criminal sanctions under the Brazilian law), consumers of digital health products are also protected under consumer laws in general and the Civil Framework of the Internet. Consumer Defence Code set forth strict liability in connection to malfunctioning and defects of products and services. It also establishes the obligation to providers to be accurate and provide transparent information about the conditions of use and safety specifications. Furthermore, in the absence of provisions regulating liabilities arising out from the use of new technologies such as AI and Machine Learning, providers will assume all risks connected to the use of such technology in association to products and services commercial claims. For more information, please refer to section 3 above.

9.2 What cross-border considerations are there?

From a Data Protection perspective, we note that the LGPD sets forth specific standards for international transfer:

a) international personal data transfer is allowed to countries or international organisations that provide a standard of protection that is comparable/adequate to the provisions set forth under the LGPD (article 33, I, of the LGPD); or

b) it is also allowed when the controller guarantees the standard of protection indicated above by means of: (i) specific contractual clauses for a determined transfer; (ii) standard contractual clauses; (iii) binding corporate rules; and (iv) according to specific standards, certificates and codes of conduct (article 33, II, of LGPD).

Additional hypotheses are set forth such as: (v) for international prosecution according to international agreements; (vi) to protect the life of the data subject; (vii) when authorised by the National Agency of Data Protection ("ANPD"); (viii) if the transfer results in a commitment set forth in an international cooperation agreement; (ix) if necessary for the execution of public policies; (x) by means of specific consent given by the data subject; and (xi) when necessary to comply with a regulatory requirement, when necessary to the execution on an agreement or preliminary procedures of an agreement in which the data subject is part, requested by the data subject; or (xii) for the exercise of legal rights in a judicial, administrative and arbitral procedure (article 33, III-IX).

The ANPD still has to provide additional considerations regarding the definition of the above-mentioned Brazilian standard of protection, but proper structure for international transfers must be in place or, otherwise, digital health companies could be subject to penalties related to the violation of LGPD.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services for data storage are usually hired in order to provide the most efficient and inexpensive information management. Companies must, under the LGPD, observe if there is any international transfer required when storing data in a multinational/foreign service provider's server (e.g. Amazon Web Service), which will lead to specific provisions of the national data protection legislation as indicated in question 9.2 above. In addition, digital health companies can be liable for data breaches and exposure of sensitive data. Therefore, proper security measures should be in place.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Companies need to consider that Brazilian legislation on the subject is still under development, in addition, it is necessary to observe issues related to confidentiality, data privacy and information security.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

Venture capital and private equity firms should consider that the legislation applicable to digital healthcare is still under development, so, sensitive issues related to confidentiality, data privacy and information security are the responsibility of digital platform providers, who should be concerned with the extent of their responsibilities considering the nature of the product or service offered.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Ana Karina E. de Souza is a specialist in Infrastructure and Energy, with a focus on projects and transactions involving private investment in regulated sectors, including concessions and privatisations, administrative and regulatory law, and project finance. A large part of Souza's work encompasses providing clients with legal assistance on investment opportunities in the regulated sectors, structuring and developing projects, providing assistance on biddings and regulated sector acquisitions, as well as general support regarding infrastructure projects. Souza has previous experience in the provision of legal assistance to clients of several areas of knowledge, such as energy, oil and natural gas, mining, transports, sanitation and pharmaceutical.

Machado Meyer Advogados
Av. Brigadeiro Faria Lima
3144 Jardim Paulistano
São Paulo – SP, 01451-000
Brazil

Tel: +55 11 3150 7702
Email: anakarinasouza@machadomeyer.com.br
URL: www.machadomeyer.com.br/en

Diego de Lima Gualda has great experience as in-house counsel in the internet, technology and digital media areas, with a deep knowledge on the sector's business models. He consolidates law expertise in different areas related to the business regarding internet and technology; marketplaces and online to offline models; freedom of speech; content removal and civil liability on the internet; privacy and data protection; intellectual property and copyright; law enforcement; strategical litigation; business development; and negotiations and contracts.
He supports companies and executives in the intersection between business, law and technology. Among other services, he provides consultancy and assistance in the implementation of programmes for law enforcement and personal data protection; regulatory consultancy and product liability (including in the legal analysis of business models and new products, as well as in the development and review of terms of service and privacy politics); consultancy on intellectual property and copyright; and support for negotiations and development of technology contracts.

Machado Meyer Advogados
Av. Brigadeiro Faria Lima
3144 Jardim Paulistano
São Paulo – SP, 01451-000
Brazil

Tel: +55 11 3150 7774
Email: dlgualda@machadomeyer.com.br
URL: www.machadomeyer.com.br/en

Elton Minasse is a specialist in technology, franchise, distribution, sponsorship, copyright, brands, patents, and software. His practice is focused on the structuring, reviewing of terms and implementation of transactions involving such matters, including the development of innovative business models and legal assistance to international clients initiating activities in the country. He has previous experience in areas of knowledge such as automotive, banking, electronic commerce, electronics, logistics, and retail.

Machado Meyer Advogados
Av. Brigadeiro Faria Lima
3144 Jardim Paulistano
São Paulo – SP, 01451-000
Brazil

Tel: +55 11 3150 7652
Email: eminasse@machadomeyer.com.br
URL: www.machadomeyer.com.br/en

Carolina de Souza Tuon is an expert on administrative law with a focus on electric power. Tuon offers consultancy on structuring, revision of terms and implementation of merger and acquisition operations and supports the mapping of the different models adopted in infrastructure projects. She also offers consultancy to foreigners who will start their activities in Brazil and acts on administrative litigation. She has experience in advising clients in various sectors, such as agribusiness, services, and power.

Machado Meyer Advogados
Av. Brigadeiro Faria Lima
3144 Jardim Paulistano
São Paulo – SP, 01451-000
Brazil

Tel: +55 11 3150 7614
Email: ctuon@machadomeyer.com.br
URL: www.machadomeyer.com.br/en

Machado Meyer has been building its history for more than 45 years, inspired by sound ethical principles, the technical skills of its professionals, and a close relationship with its clients. The firm is ranked as one of the major law firms in Brazil, with over 700 professionals.
Machado Meyer provides innovative legal solutions, anticipates scenarios and makes business possible. Combining expertise in various areas of law, broad knowledge of legislation and a thorough understanding of the matter, professionals go beyond simple problem-solving to create and preserve value for companies. Because of the significant flow of today's existing investment, the firm has organised professionals specialised in advising clients abroad and creating multidisciplinary groups, especially in Germany, Latin America and Iberian Countries, and Asia with its special desks. In other words, we work doggedly to offer intelligent legal solutions that contribute to the business growth of our clients and transform realities.

www.machadomeyer.com.br/en

© Published and reproduced with kind permission by Global Legal Group Ltd, London

China


Xun Yang


David Pan

Llinks Law Offices

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no uniform definition of "digital health" under the PRC legal framework. Medical practitioners generally believe "digital health" to be "an innovative way of healthcare that utilises the Internet and information technology in providing healthcare services". Digital health typically includes the digitalisation of therapeutics, pharmaceutical supply chains, insurance and benefits, genomics, consumer health and wellness, primary care and specialty care, imaging and other diagnostics, clinical tools and drug research and development (R&D).

1.2 What are the key emerging technologies in this area?

The key emerging technologies in digital health include big data analytics, Artificial Intelligence (AI), mobile health (mHealth), robotics, 3D printing, blockchain, augmented reality, etc. Take AI as an example, AI-based automation for image analysis promotes efficiency and productivity for radiologists, and augmented reality is re-shaping surgeries by revolutionising efficiency and cost optimisation.

1.3 What are the core legal issues in health care IT?

Among others, personal information protection and lawful utilisation of personal information is one core legal issue in healthcare IT. Since the operation of healthcare information technologies rely heavily on the collection and processing of personal information, companies in digital health business may have the ability to collect and process a significant amount of personal information, which incurs risks of such personal information being misused. Such misuse includes the excessive amount of personal information and utilisation of such information outside of the scope of purpose to which data subjects have given consent.

Additionally, stability and reliability of healthcare IT is critical to the quality of healthcare services using the healthcare IT. A failure of or an error in healthcare IT may affect personal lives or health conditions. Therefore, product safety and product liability is another core legal issue in healthcare IT.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The core healthcare regulatory schemes in China are as follows:

- Regulations for Medical Institutions on Medical Records Management (2013).
- Administrative Regulations on Human Genetic Resources.
- Administrative Regulations on Population Health Information (Tentative).
- Administrative Regulations on Application of Electronic Medical Record (Tentative).
- Drug Data Administration Law.
- Administrative Measures on Standards, Security and Services of National Healthcare Big Data (Tentative).
- Telemedicine Service Administration Regulation (Tentative).
- Administrative Measures for Internet-based Diagnosis (Tentative).
- Administrative Measures for Internet Hospital (Tentative).
- Opinions of the General Office of the State Council on Promoting the Development of "Internet plus Healthcare".
- National Standard of Information Security Technology – Guide for Health Information Security.

2.2 What other regulatory schemes apply to digital health and health care IT?

The following schemes apply to digital health and healthcare IT:

- Cybersecurity Law.
- National Standard of Information Security Technology – Personal Information Security Specifications.
- National Standard of Information Security Technology – Baseline for Multi-level Protection Scheme of Cybersecurity.

2.3 What regulatory schemes apply to consumer devices in particular?

The following regulatory schemes apply to consumer devices:

- Tort Liability Law.
- Consumer Rights Protection Law.
- Product Quality Law.
- E-commerce Law.
- Regulations on Supervision and Administration of Medical Devices.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The principal regulatory authorities in China are the following:

- The National Health Commission (国家卫生健康委员会, NHC) takes charge of national health regulation and supervision. The NHC is responsible for: formulating and carrying out administrative measures for medical institutions and the medical services industry; setting up an assessment and supervision system for medical services; and drawing up and carrying out service norms and standards for medical institutions as well as the rules of practice and service norms for health professionals.
- The National Medical Products Administration (国家药品监督管理局, NMPA), affiliated to the State Administration for Market Regulation (SAMR), supervises the safety of drugs, medical devices and cosmetics. They organise and guide the supervision and inspection of drugs, medical devices and cosmetics, develop the inspection system, investigate and punish illegal activities during the registration and manufacturing process for drugs, medical devices and cosmetics.
- The State Administration for Market Regulation (国家市场监督管理总局, SAMR) is responsible for market regulation. In the field of digital health business, various offices under SAMR exercise powers and authorities in advertisement, anti-commercial bribery and other anti-unfair competition activities.
- The National Administration of Traditional Chinese Medicine (国家中医药管理局, NATCM), affiliated to the NHC, carries out its duties within the field of traditional Chinese medicine, supervises and coordinates the integrated traditional Chinese and Western medicine work in medical treatment and research institutions.
- The National Healthcare Security Administration (国家医疗保障局, NHSA) promulgates policies, standards, statistics, regulations and guidance in the sector of healthcare and social services. The NHSA also assumes the responsibility of establishment and improvement of new rural cooperative medical systems, price controls of pharmaceuticals and medical services.
- Cyberspace Affairs Commission (国家互联网信息办公室, CAC) works jointly with the NHC and the Ministry of Science and Technology (科学技术部, MST) in regulating specific categories of healthcare-related personal information. The CAC is responsible for: the prevention of encroachment upon privacy and personal information; the medical, health and family planning service agencies under the NHC are in charge of administrating the population health information; while the MST regulates the collection, storage, study, transmission and other use of the human genetic resources.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The following points outline the key areas of enforcement when it comes to digital health and healthcare IT:

- Personal information security and protection of personal privacy has been receiving ever increasing attentions from various governmental departments. A large amount of healthcare products collect personal information via apps. In early 2019, CAC, Ministry of Industry and Information Technology, Ministry of Public Security, and State Administration of Market Regulation jointly issued the *Announcement on Special Operations against Unlawful Collection and Use of Personal Information through Apps*. In the meantime, the National Information Security Standardization Technical Committee, China Consumer Association, China Internet Association and the China Cyberspace Security Association were appointed to work together as the "App Special Taskforce", and to periodically assess the personal information collection and use status of apps on the market which have massive numbers of users and are closely related to the people's life, including those digital healthcare apps.
- PRC laws impose on all network operators the obligations to implement a multi-level protection scheme (MLPS). Since digital health providers possess and process abundant health-related data, it is critically important for health providers to enforce network operation security. Failure to complete the MLPS grading process could lead to administrative penalties. The applicable regulations and guidelines include the *Cybersecurity Law* (CSL), the *Law on Guarding State Secrets, the Regulations on Cybersecurity Multi-Level Protection* (MLPS 2.0, the exposure draft of which was issued in June 2018), and the Information Security Technology – Baseline for Cybersecurity Classified Protection.

According to the *Administrative Measures on Standards, Security and Services of National Healthcare Big Data* (*Tentative*), platforms running health/medical big data must implement MLPS, and hospitals equipped with big data technologies are generally graded as Grade III under the MLPS regime. Also, as stipulated by the *Administrative Measures for Internet Hospital* (*Tentative*), platforms which internet hospitals operate on should be graded, protected and maintained as Grade III under the MLPS regime. Other entities which engage in digital health and healthcare IT businesses are required to strictly follow the directions provided by the MLPS 2.0 to assess, grade and maintain relevant information systems.

- Export and sharing restrictions on special types of data. Specifically: (1) According to the *Administrative Regulations on Population Health Information* (*Tentative*), if any personal medical information constitutes population health information, public medical institutions at all levels must not store such data on overseas servers, and must not host or lease such servers outside the country. Also, enterprises and individuals that use population health information or provide technical maintenance and support services for population health information need to abide by relevant regulations in the *Administrative Regulations on Population Health Information* (*Tentative*). (2) According to *Administrative Regulations on Human Genetic Resources*, if personal medical information constitutes human genetic resources, foreign organisations, individuals and institutions established or actually controlled by them may not possess such information. (3) According to the *Cybersecurity Law* and relevant supporting regulations on data export requirements, if personal medical information constitutes "important data", critical information infrastructure operators must store such personal medical information within China. If it is truly necessary to provide such personal information or important data abroad, the network operator shall conduct a security assessment.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

The following regulations apply to software as a medical device:

- The *Regulations on Supervision and Administration of Medical Devices* provides the approval and clinical use regulations

© Published and reproduced with kind permission by Global Legal Group Ltd, London

on software as medical devices. Specifically, the *Rules for Classification of Medical Devices* regulate the classification of medical devices including software for medical use.

- In the context of the continuous integration of digital technology and the medical industry, the former State Food and Drug Administration issued the *Guiding Principles for the Technical Review of Mobile Medical Device Registration* in 2017. Software for medical use is included in the scope of mobile medical devices. The State Food and Drug Administration issued the *Medical Device Production Quality Management Specifications – Appendix of Independent Software* in July 2019, further strengthening the special supervision of independent software medical devices.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Obtaining applicable and appropriate telecommunication access permits, as well as protection of personal information and privacy.
- **Robotics**
  Following national and industrial mandatory and suggestive standards in R&D and manufacturing of medical robots; identifying and allocating liabilities arising from medical incidents caused by the use of robotics.
- **Wearables**
  Certain wearables with medical diagnosis or analytical functions may be deemed as medical devices under the PRC law, and therefore the marketing and sales of such wearables will be subject to government approval of medical devices.
  Personal information protection is also an important issue because most often wearables consistently collect, process and transmit personal information, most of which is personal sensitive information.
- **Virtual Assistants (e.g. Alexa)**
  Obtaining applicable and appropriate telecommunication permits, as well as protection of personal information and privacy.
- **Mobile Apps**
  Certain Apps with medical diagnosis or analytical capabilities may be deemed as medical devices (together with the smart phone or other devices they are built in) under the PRC law, and therefore their marketability will be subject to government approval of medical devices. Other important issues include obtaining applicable and appropriate telecommunication permits, as well as protection of personal information and privacy.
- **Software as a Medical Device**
  Similar to wearables and apps, certain software with medical diagnosis or analytical capabilities may constitute medical devices (together with the devices they are embedded in) under the PRC law, and therefore will be subject to government approvals applicable to medical devices. Other important issues include protection of intellectual property rights and protection of personal information and privacy.
- **AI-as-a-Service**
  Obtaining applicable and appropriate telecommunication permits, as well as protection of personal information and privacy. Additionally, product liability is also an issue because discrimination or analytical errors caused by information asymmetry between AI businesses and personal information subjects may significantly affect the quality of the service and even individual health conditions.
- **IoT and Connected Devices**
  Integrity and data security is the most important issue with regard to IoT and connected devices, as IoT consists of millions or even billions of connected devices, and hacking or breach of any part of the IoT may jeopardise a much larger scope of network and devices. Besides, lawful collection and the processing of personal information is also a big issue.
- **Natural Language Processing**
  The protection of personal information is important in natural language processing because a large amount of personal data from verbal sources need to be fed to natural language processing in order to enable the functioning. Sometimes data subjects are unaware of the personal data to be collected and fed, thus causing personal information violation concerns.

3.2 What are the key issues for digital platform providers?

In terms of the healthcare sector, digital platform providers are highly regulated. Depending on the nature and the services offered, different issues exist for different types of digital platform providers. For example, digital platform providers that provide online clinic registration services must obtain "B-25" telecommunication permits; digital platform providers that offer online diagnosis services must, in addition to "B-25" telecommunication service permits, obtain another telecommunication "ICP licenses". If drugs or medical devices are recommended or advertised during such online diagnosis services, service providers must obtain an Internet Drug Information Service Permit as well. Digital platform providers that sell drugs or medical devices online are subject to "electronic data interexchange licenses" and must obtain permits for selling drugs or medical devices online.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

CSL sets forth general rules of collecting and using personal data. All network operators, when using personal data, must strictly observe the requirements in relation to data protections.

For example, without limitations: 1) informed consent must be properly obtained from the personal data subject before collection; 2) full-lifecycle practice of personal data must comply with the mandatory principles of "legitimacy, rightfulness and necessity"; 3) personal data must be adequately protected (e.g. encryption and access management and logging); and 4) if the use of personal data exceeds the scope of prior given consent, the subject's consent must be re-acquired accordingly.

4.2 How do such considerations change depending on the nature of the entities involved?

If personal data in use is obtained from or shared by a third party, rather than directly from data subjects, the operator must ensure that such third party has duly informed the data subject of the use and sharing, and that consent by the data subject has been obtained.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Special requirements apply to specific entities which use personal data. Network operators must have a legitimate reason for the use of personal data; use of personal data must at all times be performed within the scope of the legitimate reason; where personal data is used in distributing targeted advertisements, the targeted subject should have a right to opt out.

4.3 Which key regulatory requirements apply?

When collecting personal data, digital health providers must follow the principles of "legitimacy, rightfulness and necessity". To be precise, the providers must announce the purpose, methods and scope of collection and use of personal data through the privacy policy or by other means, and must obtain the informed consent of the data subject.

If personal data is shared by pubic medical institutions, the recipient must establish a firewall of protecting the patient data received and take effective desensitisation measures to ensure that the data received cannot be used to identify a specific individual.

If a company deals with any personal data which constitutes information of human genetic resources, the company must: (1) conduct an ethical review in accordance with relevant state regulations; (2) obtain prior informed consent of human genetic resources providers; and (3) comply with the State Council's scientific technical specifications developed by the technical administration.

4.4 Do the regulations define the scope of data use?

CSL generally applies to the use of personal data which is processed electronically and manually (physical form). The principles reflected in the CSL on collection and use of personal data limit the scope of data use.

Furthermore, the National Standard of Information security technology – personal information security specifications – provides detailed guidance on scenarios, presumptions and scope of data use in various contexts.

4.5 What are the key contractual considerations?

Where the personal data in use is obtained from or shared by a third party, rather than directly from the data subjects, the user must have a data sharing agreement signed with the third party, in which such third party undertakes to have announced the purpose, methods and scope of collection and use of personal data through the privacy policy or by other means to the data subjects, and to have obtained the informed consent of the data subjects.

When a company hires a third party in the course of personal data use, for example, data processing and analysing and user-based marketing services, the company must enter into a data processing agreement with the third party. Such agreement must specify certain requirements on the data processor laid down by the CSL and the National Standard of Information security technology – personal information security specifications in relation to data protection. That is, the data processor can only process personal data on documented instructions, and the data processor must take the necessary measures to protect the personal data.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

First of all, the sharing of personal data must have been notified to and consented to by the subjects of the shared personal information. Under the CSL, the collection and processing of personal information can only be carried out with personal information subjects' informed and explicit consents. To meet this requirement, at the phase of collection, if the collector contemplates a sharing of the personal information collected, it must explicitly inform the personal information subjects (via privacy policy, other contracts, pop-up notifications in apps, or otherwise) of the purpose, method, scope and recipients, and must obtain their consent.

Secondly, personal information subjects' consent does not suffice for a full compliance. Besides the prerequisite of informed consent, CSL mandates that the collection and use of personal information must meet the criteria of "legitimacy, rightfulness and necessity". Take the element of "necessity" as an example, even if the personal information subjects have given their explicit consent to the sharing of their personal information, if the sharing to be made by the collector is unnecessary considering the business needs of the collector, the personal information subject's consent would not serve as a valid defence under the CSL for the collector's liability for its violation of the CSL.

Thirdly, if personal information will be shared outside of China, rules on data cross-border transfer will apply. Under the current PRC legal framework, Critical Information Infrastructure Operators (CIIO, defined as companies in critical sectors such as public communication and information services, energy, transportation, water utility, finance, public services and e-government, as well as other companies' destruction, malfunction or data breach of which may significantly harm national security, social welfare or public interest) must store within the Chinese territory, personal information which they collect or generate in China, and must conduct a security assessment before they transmit any personal information outside of China. Therefore, business operators in the aforementioned critical sectors or otherwise of significant importance should assess whether they constitute CIIOs. If so, such operators must conduct a security assessment pursuant to the CSL before sharing personal information with foreign parties.

Lastly, in addition to the CSL, which generally regulates personal information protection, there are special laws and regulations that regulate personal information sharing in specific sectors, for example, the financial sector and healthcare sector. Therefore, business operators in such sectors must comply with these special laws and regulations when sharing personal information outside of China, even if they do not constitute CIIOs.

5.2 How do such considerations change depending on the nature of the entities involved?

As stated in question 5.1 above, a data sharer must evaluate itself being a CIIO or a non-CIIO. A CIIO must store within China the personal information which they collect or generate within China, and must conduct a security assessment before sharing personal information with foreign parties, whereas a non-CIIO is generally free of the aforementioned legal restrictions. Next, a data sharer being a non-CIIO must evaluate whether it engages

© Published and reproduced with kind permission by Global Legal Group Ltd, London

in the business in certain special sectors, for example, the financial sector and healthcare sector. If yes, the data sharer must comply with regulations applicable in these special areas, while a data sharer being a non-CIIO which does not fall within those special business sectors is not generally bound by those special regulations.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please refer to our answer to question 5.1.

6 Intellectual Property

6.1 What is the scope of patent protection?

PRC Patent Law protects invention patents, utility model patents, and design patents. An invention patent refers to an innovative technical solution on a product, a process, or an improvement thereon; a utility model patent refers to a practical innovative technical solution to a design, structure, and combination of a product; and a design patent refers to an artistic and practical design which is suitable for industrial applications of design, drawing, pattern, colour, or a combination thereof. The following matters are not patent eligible: (1) scientific discoveries; (2) rules and methods for mental process; (3) methods for diagnosis and treatment of diseases; (4) new species of animals and plants; (5) new substances from nuclear transformations; and (6) two-dimensional designs used primarily for identifications.

In the life science sector, compounds, dosages, and usages of new drugs as well as new manufacturing processes are within patent protections; new designs of medical devices are also patent eligible. In certain cases, the shape of pills and the design of bottles for lotions as well as medical instruments are protected by design patents.

Software itself is not a patent protectable subject matter. However, the technical solution embedded in software could be patent protected. More specifically, although the coding of software or the media containing software is not a patent protectable matter, if the software is used to realise a technical solution and to achieve a certain technical result, such technical solution is a patent protectable subject matter.

Patents need to be approved in order to be granted and protected. For invention patents, the protection period is 20 years, and for utility model and design patents, the protection period is 10 years, all calculating from the application dates.

6.2 What is the scope of copyright protection?

The PRC Copyright Law protects a wide range of literary, artistic, scientific, and engineering works, including literary works, music, performances, drawings, architectures, photographs, audio and video, engineering drawings, and computer programs. Wherein, copyrightable software includes the source codes, objective codes, and the technical documentations. Database is not a standalone copyright protectable subject. However, to the extent that the selection, indexing, or grouping of data is creative, the relevant database can receive copyright protection as a compilation work. Copyright protects the expression of the works but not the ideas behind the works.

In the life science sector, typically, the manuals for medical instructions, musical therapies and the software for operating medical devices are copyright protectable.

Copyright does not need to be approved or registered. It is automatically granted upon the creation of works. However, especially with respect to computer software, a filing with the copyright protection centre will render better protections. For copyrighted works owned by companies, the protection period is 50 years from the first publication.

6.3 What is the scope of trade secret protection?

The PRC Anti-Unfair Competition Law protects trade secrets which refer to information which is kept in secret by proper measures adopted by the information owner and may bring benefits to the information owner. Trade secrets include technical secrets and operational secrets: the former refers to technical solutions and know-how and the latter refers to business plans, financial data, customer information which is kept in secret. Trade secrets can be protected for an unlimited period of time as long as they are kept secret. However, trade secret protections do not prevent any other party from independently developing or generating the same technical solution or information as those protected under trade secrets.

In the life science sector, processes for manufacturing compounds, ingredients for drugs, and parameters for medical devices could be protected as trade secrets. Additionally, source codes of computer software may be protected as trade secrets.

6.4 What are the typical results on academic technology transfer rules?

The government encourages universities and research institutions to transfer, license, or otherwise to commercialise their technological achievements. The professors and researchers who contribute to technical achievements are entitled to rewards and remunerations at the amount agreed with the universities and research institutions or, absent such agreement, at the amount of a statutory percentage of the benefits which the universities or research institutions receive as the results of the transfers, licences, and commercialisations.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Software can be approved as a medical device if it itself has a medical function and can run on a generic computer platform. If a software can only worked on a specific device, the device can be approved as a medical device together with the software.

Like other software programs, software as a medical device receives copyright protections and the technical achievement embedded in it may be patented.

Additionally, clinical data in relation to the clinical trials of the device receive data exclusivity protections.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Generally speaking, under the PRC laws, a party owns and enjoys the intellectual property rights it develops. Under a collaborative arrangement, unless otherwise agreed, it is the party which develops the improvement, not the one which contributes the background technology or provides resources, that owns the improvement. For example, when a pharmaceutical company

© Published and reproduced with kind permission by Global Legal Group Ltd, London

engages in a hospital to perform clinical trials, unless otherwise agreed, it is the hospital that owns the achievements out of the clinical trials. If both collaborative parties contribute to an improvement, the default rule is that they own the improvement jointly.

A notable exception is scientific research in relation to human genetic resources. A foreign party must partner with a Chinese party in performing such researches to the extent human genetic resources originated from China is used and the parties must own the achievements out of the research jointly regardless of whether the Chinese party actually contributes to the development.

Additionally, it is worth noting that if personal data are involved in the research, the data can be shared among collaborative parties only if data subjects' consents are secured.

7.2 What considerations apply in agreements between health care and non-health care companies?

It is customary for healthcare companies to collaborate with specialist vendors to improve their business or to outsource part of business functions, including in particular, IT service providers. Note that licensed activities, e.g., medical services, must not be outsourced. Additionally, when outsourcing the process of patient data or other health-related data, the healthcare company must adopt proper measures to ensure that the processor meets the data protection standard which the law requires and it comments to the data subjects; and will still be primarily responsible for the security of the data.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning in digital health is generally used in the following areas:

- AI-aided diagnosis and treatment, especially AI technology used in medical imaging.
- Genetic test and risk prediction, which provides AI-based analysis of genetic test to predict the potential risk of different diseases.
- Individual healthcare management, which provides an individualised health management plan based on individual health information conditions based on AI technology.
- Hospital management, which optimises the process of hospitals' operations, including patients' management, based on AI technology.

8.2 How is training data licensed?

Existing cases show that data can be licensed as if they are a type of intellectual property. All the legal requirements and other considerations in relation to licences of technology apply.

Additionally, if personal data are involved, the licence of data will be subject to data subjects' consents and to security considerations.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Algorithms are not patentable and they are not protected by copyright either. They may be protected as trade secrets if they are kept confidential. Copyright protection is available for software programs which reflect algorithms (i.e., the expression of algorithms).

It remains controversial as to whether achievement made by AI receives intellectual property protections because, strictly speaking, both copyright law and patent law protect only human creations. However, recent cases indicate the trend that the party which runs the AI has the chance to receive protections over the achievements made by the AI it operates.

8.4 What commercial considerations apply to licensing data for use in machine learning?

As for a normal licence of technology, typical commercial considerations for a licence of data includes: scope of use; exclusivity; warranties; and rights in the achievements arising from machine learning, etc. Additionally, if the relevant data contain personal information, individual consents are required.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Under PRC laws, both medical service providers (e.g. clinics and hospitals) and medical device manufacturers are responsible for adverse outcomes out of digital health services.

Medical service providers are preliminarily responsible for the adverse outcomes out of the medical treatment activities. In accordance with Art. 54 of the *PRC Tort Liability Law* (the "**Tort Law**") effective in 2010, in any event that a patient sustains any harm during the course of diagnosis and treatment due to the negligence of the medical service providers, the medical service providers are liable for the damage incurred by such patient. Typical examples of "negligence" in digital health services include violations of applicable healthcare laws and regulations, healthcare professional's malpractices, improper treatments, etc.

The PRC has specific rules on liabilities out of the provision of "remote medical consultations" and of "remote diagnosis and treatment" which are considered two types of legally recognised remote medical services. The former refers to the arrangement where a medical service provider consults another medical service provider remotely in providing medical services, whilst the latter refers to the arrangement where a medical service provider invites another one to perform diagnosis and treatment together. Pursuant to the *Managerial Specifications on Remote Medical Services* issued jointly by the National Health Commission and the National Administration of Traditional Chinese Medicine in September 2018, with respect to remote medical consultations, the medical service providers which directly face patients are solely responsible for any claims raised by patients out of such services; whilst, with respect to remote diagnoses and treatments, both the medical service providers which offer and those which accept the invitation for joint remote diagnoses and treatments are held jointly liable for any disputes arising therefrom or in connection of such services.

If the adverse outcome is attributable to defects in the medical device, the manufacturer is primarily responsible for the losses and damages which patients suffer during the course of diagnosis and treatment on a strict liability basis. According to the Tort Law and the *PRC Product Quality Law*, if any damage or harm to a patient is caused by the defects of medical devices, the manufacturer must compensate, jointly with the relevant medical institution, the said patient without considering whether such manufacturer is at fault.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

9.2 What cross-border considerations are there?

With respect to medical services, only domestic registered medical service providers (either domestically or foreign invested) are allowed to provide medical services in the PRC. Such a service provider is allowed to consult another medical service provider (either inside or outside of China) when providing medical services and it takes primary responsibility for the services. Foreign medical service providers are unable to obtain the licence to offer medical services in the China market.

With respect to the medical device which has a remote healthcare function, the agent that imports the device takes the primary responsibility. According to the *Administrative Measures for the Registration of Medical Devices* (the "**Medical Devices Registration Measures**") effective since 2014, if a foreign company wishes to export its medical devices to China, it must apply for a regulatory approval through an "agent" residing in China. The "agent" could either be its subsidiary in China or a qualified Chinese company. According to Art. 14 of the *Medical Devices Registration Measures*, the agent will take stringent responsibility, jointly with the foreign company which produces the medical device, for the quality and after-sale services in relation to the medical device.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

China does not have any rule specific to digital healthcare services based on the Cloud. However, general cyber security rules apply.

With respect to medical services, although there is no law or regulation which prohibits the provision of medical services on the Cloud, it would be difficult to structure a cloud-based medical service business because, generally speaking, electronic medical records are not allowed to be stored on any server other than those in possession and control of the relevant medical service providers.

With respect to medical devices, the regulator has approved a number of medical devices which operate with a cloud-based data centre. The security and stability are key issues the government looks into when granting the regulatory approvals.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

China has the largest Internet population and a fast-developing internet business. The government encourages the application of internet technologies to the healthcare sector to resolve the shortage of good-quality medical resources. Consequently, many internet companies expanded their business into a digital healthcare sector.

However, please note that both the telecoms business and the healthcare business are highly regulated. Internet companies which wish to enter into healthcare business must seek another operational permit. Generally speaking, a company must have a physical site to operate as a hospital in order to provide medical services according to the *Managerial Rules for Internet Hospitals (Trial)* (the "**Internet Hospital Rules**") issued in 2018. The establishment of an internet hospital must be approved by the regulator and technology companies are prohibited from engaging in the internet hospital business, unless a qualified medical institution is jointly liable for the establishment and operation of such internet hospital.

Medical device business is regulated too. The same as other medical devices, the manufacturing, distribution and marketing of remote-connected medical devices require regulatory approvals. Additionally, since the device needs to be connected to public networks in order to be functioning, a network access permit is also required.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

For remote healthcare business, depending on the business model, operational permits for healthcare business and for telecoms business may be required. During the application for these permits, relevant regulators will review, among other factors, the shareholders and the equity structure. When there is any change in shareholders and in the equity structure, e.g., venture capital and PE firms' entrance into, and exiting of the digital healthcare business, the operational permits will likely be revisited.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Xun Yang is a partner at Llinks Law Offices, focusing on IP/IT practice, including IP protections, cyber security, and regulatory matters as well as investment in the high-tech areas. He graduated from Fudan University with both a Bachelor's in law and a Master's in law. He also received an LL.M. degree from Columbia University.
Prior to joining Llinks, Xun gained previous experience of working for renowned international law firms such as Freshfields Bruckhaus Deringer and Simmons & Simmons, based in Shanghai, Hong Kong, London and other international cities for a total of 15 years, of which almost eight years were experience in foreign jurisdictions.
Xun has been recommended by *The Legal 500* in the IP practice in 2020, in the TMT practice in 2019, and recommended by *Business Law Journal* in the Life Science sector in 2019.

Llinks Law Offices
19F, One Lujiazui, 68 Yin Cheng Road Middle
Shanghai 200120
China

Tel: +86 21 3135 8799
Email: xun.yang@llinkslaw.com
URL: www.llinkslaw.com

David Pan is a partner at Llinks' Corporate & Compliance Practice. David holds an LL.M. from Harvard Law School and a Ph.D. from Shanghai Jiao Tong University. He is admitted in both the USA and China, and has been practising law for over 18 years in both countries. David's clients span the full spectrum from global *Fortune 500* companies to local high-potential and high-growth start-ups. He regularly advises on all major corporate & compliance issues ranging from antitrust, data (cyber security, data privacy and other data-related issues), and anti-corruption (ADA). In addition to ADA, David advised major transactions in the healthcare business sector such as M&A, in-and-out technology licensing and market authorisation.
David is recognised in *Chambers*, *The Legal 500*, and *LEGALBAND* as a leading PRC lawyer in areas of corporate & compliance, antitrust and competition, and cybersecurity and data privacy protection, respectively.

Llinks Law Offices
19F, One Lujiazui, 68 Yin Cheng Road Middle
Shanghai 200120
China

Tel: +86 21 3135 8701
Email: david.pan@llinkslaw.com
URL: www.llinkslaw.com

Llinks Law Offices is a leading PRC law firm, reputable for its high quality and specialised services, as well as innovative and practical solutions. Llinks has lawyers focusing on both life science and TMT sectors, covering a wide array of practice, including regulatory, intellectual property, compliance, FDI and M&A and data protections. Llinks' life science focus group and TMT focus group has recently joined efforts in serving clients in digital health areas. Llinks advises both pharmaceutical and medical device companies which move their business online and TMT companies which expand their business to the life science sector. Llinks also serves PEs and VCs which invest in digital healthcare business.
Llinks is consistently recognised as a leading Chinese law firm by various reputable legal rating agencies such as *Chambers*, *The Legal 500*, *IFLR1000*, *Asia law Profiles*, and have been recommended in both the TMT and life science sectors.

www.llinkslaw.com

LINKS Law Offices 通力律师事务所

© Published and reproduced with kind permission by Global Legal Group Ltd, London

France


Anne-France Moreau, Counsel


Lorraine Maisnier-Boché, Associate

McDermott Will & Emery

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

"Digital health" is not defined under French law. The French Public Healthcare Code (**FPHC**) exclusively refers to "*telemedicine*", defined as a "form of remote medical practice by means of information and communication technologies, which brings one or more healthcare professionals (**HCPs**) together or with a patient, and, where appropriate, other professionals involved in the patient's care" (Art. L. 6316-1 FPHC), consisting in teleconsultation, tele-expertise, tele-monitoring, tele-assistance and medical regulation) (Art. R. 6316-1 *et seq.* FPHC). Various other terms are used by French authorities to refer to concepts related to "digital health"; although they are not strictly defined, they all refer to the digital revolution in healthcare to enable patients and HCPs to (i) better monitor, manage and improve healthcare, (ii) reduce inefficiencies in the delivery of healthcare, and (iii) improve access to treatment and HCPs by reducing costs, increasing quality and personalising healthcare.

1.2 What are the key emerging technologies in this area?

Due to the universal access to mobile networks and the increasing use of smartphones, mobile health applications, and notably connected medical devices (**MD**), are among the key emerging, widely spreading technologies in this area. Healthcare IT solutions intended for HCPs (e.g. clinical decision support, machine learning or predictive analyses) and/or patients (e.g. teleconsultation platforms, webchat for symptom checking, online pharmacies) are examples of booming IT health products. The French government demonstrated its commitment to foster the development of artificial intelligence (**AI**) in the field of healthcare by launching a national health database (*Health Data Hub*) on 1 December 2019.

1.3 What are the core legal issues in health care IT?

- Applicable Regime: the regulatory status of a given healthcare IT product will determine the specific regime, and thus the relevant pre- and post-commercialisation considerations. At this time, the legal framework for approving AI-powered diagnostic devices is not yet settled and generally, the period for MD regulatory review has increased in Europe due to the coming into force of the new MD regulations (cf. §2.6).
- Data protection: healthcare IT is likely to involve the collection, storage, transfer and processing of (highly sensitive) personal health data, subject to the General Data Protection Regulation (**GDPR**) and the French Data Protection Act No. 78-17 of 6 January 1978. French law also provides for additional requirements specifically applicable to healthcare IT (Art. L. 1111-8 and L. 1110-4-1 FPHC, cf. §2.2).
- Regulation and reimbursement of *telemedicine*: in September 2018, the French national security scheme introduced provisions allowing for the reimbursement of certain telemedicine acts (Art. L. 6316-1 *et seq.* FPHC).

2 Regulatory

2.1 What are the core health care regulatory schemes?

European and French legislators have addressed many aspects of healthcare, ranging from relationships between industrials and HCPs, public health policy and patients' rights in cross border healthcare to the health products. At the French level, such regulations are mostly codified in the FPHC – e.g. anti-gifts and transparency provisions (Art. L. 1453-1 *et seq.* FPHC), advertisement of MD (Art. L. 5122 and L.5213-1 *et seq.* FPHC), medical ethics (Art. R.4127-1 *et seq.* FPHC), and manufacturing and distribution of medicinal products (Art. L. 5124-1 *et seq.* FPHC). Provisions from other French codes may, however, apply to specific aspects of healthcare (e.g. respect due to the human body in the Civil Code (**FCC**), reimbursement schemes in the Social Security Code (**FSSC**), etc.). Finally, regulatory agencies play an active role in the construction and implementation of guidelines, which aim to improve the comprehension of regularity schemes by the market actors (cf. §2.4).

2.2 What other regulatory schemes apply to digital health and health care IT?

- Regulations on MD: cf. §2.6.
- Regulation and reimbursement of *telemedicine*: cf. §2.6 and through the setting of good practice guidelines (HAS' guidelines published in May 2019).
- Regulations on electronic medical records (*dossier médical partagé* – **DMP**): creation of a digital health record that stores and secures patients' health data, starting in the summer of 2021 (Art. L. 1111-14 and *seq.* FPHC and R.1111-26 and *seq.* FPHC).
- Regulations on data protection: see §4.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.3 What regulatory schemes apply to consumer devices in particular?

There is no specific regulatory scheme for "consumer devices" as a standalone category. General regulations cover various aspects of the life cycle of consumer devices – e.g. the French Consumer Code addresses the relationship between professional providers and consumers; defective product liability regulations are applicable to defective consumer devices (Art. 1245 *et seq.* FCC).

The line between wellness consumer devices (e.g. diet app, sport assistant watch) and MDs with a medical purpose, which are subject to a specific regime (§2.6), may be difficult to draw.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

- **Directorate General for Care Provision (DGOS)**: reports to the French Ministry of Health and plays the role of interface with healthcare institutions. It must notably ensure quality, continuity and proximity of the care.
- **National Agency for the Safety of Health Products (ANSM)**: key agency notably responsible for authorising clinical trials, monitoring adverse reactions related to health products, inspecting establishments engaged in certain activities and authorising health product imports. The ANSM regularly publishes influential guidelines and situational analyses and may impose administrative sanctions.
- **Data Protection Authority (CNIL)**: responsible for ensuring the protection of personal data. Its role is to alert, advise and inform the public, and it also has power to control and sanction through the issuance of injunction and fines to data controllers.
- **National Health Authority (HAS)**: notably responsible for the pricing and reimbursement of health products and the optional certification of prescription assistance software. The HAS regularly publishes guidelines, some of which are specific to digital health.
- **Regional Health Agencies (ARS)**: responsible for regulation of healthcare provision at the region level, including implementation of a digital health policy.
- **National Digital Health Agency (ANS)**: responsible for assisting the State in implementing digital health regulation, specifically by issuing recommendations and guidelines regarding security and interoperability, as well as by developing health software and projects.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

- Defective MDs: the sector of MD is under close scrutiny. Manufacturers of connected implants and high-risk medical assistance software are exposed to product liability claims.
- Data Protection: digital health likely involves the processing of personal health data, considered as highly sensitive. Failure to meet data protection requirements may therefore result in severe sanctions, such as an injunction to stop the data processing or fines up to EUR 20,000,000 or 4% of total worldwide annual revenue, which can be publically issued.
- Regulatory Requirements: access to the market may depend on stringent regulatory requirements. For example, the ANSM has already suspended the placing on the market, and prohibited the distribution, of a software wrongly marketed as a consumer device when it should have been certified as a MD (ANSM Decision of 12 January 2015).

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Like other MDs, software is subject to pre- and post-commercialisation requirements (CE-marking, materiovigilance, etc.) set forth by (**i**), at the European level, Regulation (EU) 2017/745 on MD (**MDR**) or Regulation (EU) 2017/746 on *in vitro* diagnostic MD (**IVDR**) (that will enter into full force respectively in May 2020 and May 2022 and are directly enforceable in France) and (**ii**), at the French level, by the FPHC (e.g. provisions on advertisements Article L.5213-1 *et seq.* FPHC). The new regulations notably reinforce the rules on clinical performance evaluation of MDs.

To clarify this regulatory scheme, regulatory authorities have issued guidelines tailored to software as an MD (e.g. the MD Coordination Group of the European Commission issued guidelines on qualification and classification of concerned software in October 2019 MDCG 2019-11 – formerly MEDDEV guides; the HAS issued guidance on the assessment of connected MD for reimbursement purposes in February 2019).

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Depending on the telehealth product or service, different legal regimes may apply, mainly the telemedicine or online pharmacies regulatory requirements, as well as the medical devices regulations.
  Health data protection and security requirements, as well as the issue of liability and reimbursement of such products or services, are key.
- **Robotics**
  Robotics are at the crossroads of several potential legal regimes. The liability issue is of great importance and must be clearly allocated between the involved parties, and must take into account the legal regime of product responsibility. Depending on the features, medical devices regulations may also apply.
- **Wearables**
  The monitoring involved by wearables, specifically when collecting precise and daily information that can reveal health status, requires strict compliance with data protection laws. Depending on the features, medical devices regulations may also apply.
- **Virtual Assistants (e.g. Alexa)**
  The monitoring involved by virtual assistants, depending on the way they can be activated and how they record information, and use of AI technologies in order to train virtual assistants, requires strict compliance with data protection laws and security requirements and triggers some questions regarding algorithms transparency.
- **Mobile Apps**
  Data protection and security requirements, specifically for health and/or monitoring apps, as well as the issue of liability, are key. Depending on the features, medical devices regulations may also apply.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- **Software as a Medical Device**
  Medical devices, as well as health data protection, including additional public health requirements regarding interoperability and security, will apply. Proper allocation of liability is key.
- **AI-as-a-Service**
  Training an AI requires processing of large amounts of personal data and, depending on the features, of health data, triggering compliance requirements with data protection and security, specifically for sensitive data. Algorithms transparency and IT security must be ensured. Depending on the features, medical devices regulations may also apply.
- **IoT and Connected Devices**
  Data protection and security requirements, specifically for health and/or monitoring devices, as well as the issue of liability, are key. Depending on the features, medical devices regulations may also apply.
- **Natural Language Processing**
  Natural language processing is at the crossroads of AI and personal data processing. Algorithms transparency, data protection compliance, and in some cases, medical devices regulations are key. Depending on the service using such processing, the issue of illegal practice of medicine can be relevant.

3.2 What are the key issues for digital platform providers?

Providers may face specific regulatory constraints depending on the nature of the services they offer. Online sale of medicines is, for example, subject to stringent requirements under French law (only pharmacies may sell medicines; online sale is limited to over-the-counter drugs), which are strictly interpreted by French courts (see *Cour de cassation* 19 June 2019 n° 18-12.292). "*Telemedicine*" platforms may not publish advertising that conflicts with medical ethics (notably, French law prohibits medical practice as a business). By contrast, medical information platforms are not related to a medical activity *per se* and thus are subject to general regulation.

Security requirements are higher for digital health platform providers (e.g., if medical data are processed, such providers may only use the services of a certified health data hosting service provider (Art. L. 1111-8, FHPC), and must comply with IT guidelines, especially regarding health data access (Art. L. 1110-4-1, FHPC).

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Personal data are subject to the GDPR, and its key principles, mainly of lawfulness, are fairness, transparency, proportionality, purpose limitation and data minimisation, and are subject to the French Data Protection Act requirements, specifically regarding health data.

4.2 How do such considerations change depending on the nature of the entities involved?

Data protection laws apply regardless of the nature of the entities, whether public or private. However, some entities may be subject to derogations depending on the importance of the data processing operations (e.g. SMEs).

4.3 Which key regulatory requirements apply?

In order to carry out personal data processing, the data controller must implement compliance steps:

- to maintain a record of processing activities under its responsibility;
- to inform the individuals of the existence of the processing; and
- to ensure that the agreements entered into contain adequate provisions in order to properly determine capacities of the parties and allocate roles and responsibilities.

As special categories of data, health data are also subject to specific requirements under the GDPR and additional national obligations:

- processing of health data is, by principle, prohibited, except where based on a specific legal ground (such as prior and express consent, or where necessary, for purposes of preventive medicine, medical diagnosis, provision of health or social care, etc.);
- health data processing must, in addition, be justified by a public interest and be authorised by the French Data Protection Authority, unless it falls under some exceptions; and
- organisational and technical security measures must be adapted to the level of data sensitivity (encryption, access monitoring, pseudonymisation or even anonymisation).

4.4 Do the regulations define the scope of data use?

Scope of data use is determined, to the extent that the data processing must be lawful, in view of its purpose and of the conditions of implementation of the data processing operations.

Some specific restrictions must be highlighted, for instance the prohibition to sell health data that are directly or indirectly identifiable (Art. L. 1111-8, VII, FPHC), or the prohibition to use health professionals' information extracted from medical prescriptions (Art. L. 4113-7, FHPC).

4.5 What are the key contractual considerations?

Regarding business-to-business relationships, the requirement to enter into an agreement depends upon the capacities of the stakeholders:

- in a data controller and data processor relationship, an agreement must be entered into, the provisions of which are expressly defined by the GDPR (Art. 28). Security requirements are of the essence;
- in a joint data controller relationship, an agreement must be entered into (Art. 26), the provisions of which are not specifically defined. However, it is highly recommended to precisely allocate the roles and responsibilities of the parties, depending on the actual level of involvement; or
- in an independent controller relationship, an agreement is not required, but may be recommended if material personal data exchanges are taking place.

Regarding business-to-consumer relationships, the obligation for the data controller to provide relevant information to the individuals, and, in some cases, to obtain their express consent, has an impact on the contractual documents with individuals. Lack of such information may lead to the impossibility to use personal data in a lawful manner.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Data protection laws, as well as specific requirements regarding sharing of medical data, specifically where covered by medical secrecy, are applicable.

5.2 How do such considerations change depending on the nature of the entities involved?

Data protection laws apply regardless of the nature of the entities, whether public or private, except where requirements are specifically applicable to health professionals.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Sharing personal data must always be subject to entering into an agreement (cf. §4.5) and to adequate security measures during transmission.

Personal data transfers to recipients located outside the EU, in a third country that does not ensure an adequate level of protection, must be covered by appropriate safeguards, the most common of which are data transfers agreements (standard contractual clauses adopted by the EU Commission).

If data is covered by medical secrecy (Art. L. 1110-4 FHPC), a specific regime for "shared medical secrecy", it generally requires patient consent to share its medical data with any third party outside of the healthcare team (Art. L. 1110-12 FHPC).

6 Intellectual Property

6.1 What is the scope of patent protection?

As in other jurisdictions, in order to be covered by a patent issued by the French Industrial Property Office (**INPI**), an invention must be new, involve an inventive step and have an industrial application. In principle, computer programs and mathematical methods are not patentable *per se* (Art. L. 611-10 French Intellectual Property Code – **FIPC**). Abstract ideas and mathematical formulas may not be subject to patent protection. However, a computer program that produces a "technical effect" and certain AI-related inventions directed to a technical subject-matter, providing a non-obvious technical solution of a technical problem (e.g. a neural network in a heart-monitoring apparatus for detecting irregular heartbeats) may be patentable. Patents offer strong protection, but are limited in scope to the patent claims, and the protection is of limited duration (20 years). Additionally, patent protection requires public disclosure of the invention as patent application is published 18 months after filing of the patent.

6.2 What is the scope of copyright protection?

Copyright protects an original work in a fixed form (Art L.112-1 of the FIPC). Ideas, concepts or mathematical formulas may not be subject to copyright. A software's architecture, source code, object code and preparatory design material is eligible for copyright protection, but not the algorithm. In addition to economic rights, the copyrights' holder benefits from certain moral rights which are perpetual, inalienable and not subject to statutes of limitation, whereas economic rights last 70 years after the author's death or after the works' disclosure where it belongs to a legal person. The original work is protected without formalities from the day it is created, whatever its form, nature, merits or destination.

6.3 What is the scope of trade secret protection?

In 2016, European Commission enacted *Directive (EU) No. 2016/943 of 30 July 2018*. In France, information protected under trade secrets is defined as any information that is: (i) not generally known or easily reachable by specialists of the matter; (ii) of commercial value, actual or potential, because of its secret nature; and (iii) subject to reasonable protective measures by its legitimate holder to keep it secret (Article L 151-1 to L 154-1 of the French Commercial Code). Trade secret protection may apply to a company's algorithms.

6.4 What are the typical results on academic technology transfer rules?

There is no specific academic technology transfer rules scheme applying to healthcare IT. In 2019, France Biotech, an industry association, began to develop tools (negotiation process, templates, access to existing agreements) to facilitate and accelerate technology transfer and, in collaboration with BPI France, have begun to study and suggest improvements to the technology transfer process.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Intellectual property protection for Software as a Medical Device (**SaMD**) will depend on the features and functionality of the product, as well as the nature of the specific market. A particular SaMD may be protected simultaneously by more than one type of intellectual property protection (patent, copyrights, trade secret, trademarks, design).

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The main consideration is to define a clear intellectual property scheme regarding the results generated during a partnership, depending on the allocation of the responsibility between the parties as defined in the development plan. In the case of academics being involved, they frequently request joint ownership of results, independent of inventorship.

7.2 What considerations apply in agreements between health care and non-health care companies?

There are many considerations to assess in negotiating agreements in the field of digital health: ensuring business continuity with respect to the product, warranties on the compliance/regulatory capabilities, cross borders concerns and data breach indemnity.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning holds a rising position in the digital health sector, in order to assist health professionals in their daily practice as well as in research. AI can provide assistance in decision-making as well as make the decision itself, but only under very strict circumstances (e.g. express consent of data subjects).

8.2 How is training data licensed?

Training data can only be protected by intellectual property right as an entire database if it is original, or, if not, if the owner can demonstrate a substantial investment in obtaining, verifying and presenting data. In this regard, training data can be licensed, subject to compliance with regulatory requirements.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

The author of a creation is a natural person and protection automatically arises (see question 6.2). Regarding computer programs, rights may be vested in a company employing the author if the employee has acted in execution of his duties or following the employer's instructions. The European Patent Office has already refused patent applications designating an AI as inventor (January 2020).

8.4 What commercial considerations apply to licensing data for use in machine learning?

In addition to securing the necessary rights to use training data, data integrity and reliability are key considerations, as well as obtaining transparency guarantees regarding machine-learning algorithms.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

- Civil liability: the producer of the device can be found liable on the basis of defective product liability, where a person suffers harm from the use of a defective digital health product or service (e.g. if the software malfunctions or delivers incorrect results). Claims may also be brought against economic actors involved in the manufacturing and/or distribution of digital health products under fault-based regimes.
- Criminal liability: manufacturers, distributors, users and other actors involved in digital health may be liable on the ground of specific offences described in the FPHC or ordinary offences (e.g. involuntary manslaughter).
- Regulatory liability: manufacturers may be exposed to administrative sanctions imposed by regulatory authorities if they fail to meet regulatory requirements related to or resulting in adverse outcomes in digital health.

9.2 What cross-border considerations are there?

There are many cross-border considerations likely to impact the business model of industrials engaging in the field of digital health, including:

- Cross-border healthcare: Directive 2011/24/EU on patients' rights in cross-border healthcare sets out the conditions under which a patient may receive medical care from a HCP located in another EU country – it covers healthcare costs, as well as the prescription and delivery of medications and MD.
- MDs and local representation: in order to place a MD in the EU market, a non-EU manufacturer must designate an "*authorised representative*" (Art. 11, MDR).
- Transfer of data: see question 5.2.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Storage of data (see question 3.2), access and protection (data anonymisation, cybersecurity, etc.) and complying with consent withdrawal are key.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

The healthcare market is a complex sector, marked by a multiplicity of actors (industrials, HCPs, regulators, patients, social security scheme, hospitals, etc.) and a high level of normativity (regulatory barriers to entry to the market, liability exposure, etc.).

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

A threshold consideration is whether the healthcare IT will provide the necessary features, functions and tools to meet the market needs, as well as compliance and regulatory requirements with the abovementioned.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Anne-France Moreau counsels companies founded on a R&D innovation with a focus on pharmaceuticals, medical devices, digital health and cosmetic(s) industries. She assists French and non-French groups in the preparation and negotiation of partnering agreements such as collaborations, licences, manufacturing and supply agreements. She also handles regulatory matters in this respect.

McDermott Will & Emery
23 rue de l'Université
75007 Paris
France

Tel: +33 1 81 69 15 53
Email: amoreau@mwe.com
URL: www.mwe.com

Lorraine Maisnier-Boché focuses her practice on data protection and information technology (IT) law. She has deep experience in the digital and IT sector as well as the healthcare industry, frequently advising healthcare professionals, hospitals, governmental entities, insurance companies, medical device manufacturers, software editors and hosting service providers on complex IT projects. Lorraine has a strong background in data protection, and regularly advises on GDPR compliance programs, international data transfers, marketing and profiling actions, sensitive data (e.g. personal health data), audits and security issues.

McDermott Will & Emery
23 rue de l'Université
75007 Paris
France

Tel: +33 1 81 69 14 77
Email: lmaisnierboche@mwe.com
URL: www.mwe.com

Established in 1934 as a tax practice in Chicago, McDermott has grown its core practices and offices around the globe. We partner with leaders around the world to fuel missions, knock down barriers and shape markets. With 20 locations on three continents – 11 US offices, eight European offices, as well as a strategic alliance with MWE China Law Offices in Asia – our team works seamlessly across practices, industries and geographies to deliver highly effective, and often unexpected, solutions that propel success. More than 1,100 lawyers strong, we bring our personal passion and legal prowess to bear in every matter for our clients and the people they serve. Looking to the future, we will continue to expand geographically and enhance our existing practices, industry-focused practices and industry-focused strengths. We are committed to building from these strengths in order to best serve our clients and communities.

www.mwe.com

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Germany


Dr. Stephan Rau


Steffen Woitz


Dr. Karolin Hiller


Jana Grieb

McDermott Will & Emery LLP

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

German law does not define the term "digital health". Generally, the term is interpreted quite broadly. "Digital health" covers all features of health telematics infrastructure, including electronic health and patient files, electronic drug prescriptions, healthcare assistance and surveillance systems (in particular but not limited to software as medical devices (SaMD)), telemedicine services, medical consultations and treatments by means of distance communication, apps and wearables, the implementation and use of healthcare databases, as well as the use of artificial intelligence (AI).

1.2 What are the key emerging technologies in this area?

The key emerging technologies in the sector of digital health in Germany are SaMD, other apps, wearables, and features for medical treatment by means of long-distance communication. The competent German public authorities are currently working on the implementation of a functioning telematics infrastructure within a reasonable timeframe. All healthcare providers shall be obliged to sign in and offer such services to their patients/clients.

1.3 What are the core legal issues in health care IT?

The challenge is to provide a functioning and safe telematics infrastructure as soon as possible. The patients' fundamental rights of autonomy and privacy shall be respected; but high standards of healthcare services are to be guaranteed too. German Parliament and the competent authorities have to find a balance between the chance to use digital health for improving human healthcare services on the one hand, and the implementation of sufficient rules and regulations on the other hand, in order to protect human lives, health and the patients' right of data privacy, as well as to guarantee a working liability scheme.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The most relevant regulations for the digital healthcare market are the amendments to the provisions on inpatient (e.g. for hospitals and/or care homes) and outpatient (e.g. for GP practices, specialists and home care providers) care, as far as newly implemented national and European laws on medical devices and the national and European data protection law.

2.2 What other regulatory schemes apply to digital health and health care IT?

Other relevant regulations in the digital healthcare sector are the recently amended State Professional Ordinances for Physicians (e.g. permission for medical care by means of long-distance communication), laws on product and professional liability (e.g. liability for physical injuries, property damages or financial losses caused by a malfunctioning device), laws on intellectual property (e.g. protection for sensor-based monitoring systems, such as infant incubators), as well as pharmaceutical laws and drug regulations (e.g. drug dispensing after online consultation).

2.3 What regulatory schemes apply to consumer devices in particular?

Consumer devices are primarily regulated by European and national medical device law, laws on outpatient care (including reimbursement rules), and European and national data protection laws.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The self-governing associations and bodies of healthcare providers, like the Federal and State Associations of Public Health & Insurance (SHI), Licensed Physicians, the Organisation of the Private Healthcare Insurers and the Federal and State Organisation of the Statutory Healthcare Insurers, are authorised by law to regulate autonomously and specify certain fields of the healthcare sector by means of statutes, guidelines and secondary regulations. The self-governing entities are, next to the Ministry of Health, the shareholders of the *Gesellschaft für Telematik* (Gematik). Gematik is a specially created company that the legislator entrusted with the task of developing a suitable technical concept for an electronic patient health card, electronic patient files, electronic drug prescription and other electronic applications and features that shall be immediately or in the future available on the German healthcare market. Gematik is also responsible for the construction and maintenance of the required telematics infrastructure, as well as the subscription of all healthcare providers into the infrastructure within the set timeframe.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

With effect from 1 January 2020, SHI-licensed patients are entitled to prescription of those digital healthcare apps of category I and IIa, which were registered by the Federal Institute for Drugs and Medical Devices (BfArM) and the reimbursement of their costs. The registered digital healthcare apps will be one key area of enforcement along with a high standard of medical care provided by means of long-distance communication, as well as adequate measures and techniques to protect sensitive personal healthcare data.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Medical software is, under certain conditions, considered a medical device and is therefore subject to the requirements of EU medical devices directives and the related Member State laws. In contrast, medical devices do not require a genuine marketing authorisation to drugs in the EU so far. Thus, before software as a medical device (SaMD) is placed on the EU market, a medical device has to undergo a conformity assessment procedure in order to confirm that it complies with the essential requirements under the EU Medical Devices Directive (MDD). The type of conformity assessment procedure to be used depends on the medical device's risk class. Currently, most SaMD is classified as class I and is therefore subject to a basic conformity assessment procedure that does not require the involvement of a notified body. After successful completion of the conformity assessment, the manufacturer may affix the CE-mark to the product. The CE-mark entitles the manufacturer to place the product on the market in the CE-zone, which currently covers the EEA (the EU plus EFTA-countries), as well as Turkey and Switzerland.

In 2017, new EU regulations on medical devices were adopted. The new regime will become applicable on 27 May 2020 (for medical devices) and 27 May 2022 (for *in vitro* diagnostic medical devices). The new legal framework modifies the risk classification system; many devices will be classified in higher risk classes. Due to this up-classification, but also as a result of increased requirements in the conformity assessment procedure, placing medical devices on the market in the EU will become more difficult. However, the certification system will be maintained and no genuine authorisation procedure has been introduced, so that the procedure will continue to be significantly less challenging compared to drugs. Most SaMD products are currently classified in class I, though there is a high risk of up-classification. Consequently, under the new law, manufacturers of SaMD will often need CE-certificates issued by notified bodies.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Telehealth means the use of electronic information and digital telecommunication technologies to support and promote long-distance healthcare, educate providers and patients and provide health information.
- **Robotics**
  Robotics, i.e. machines that (partly) substitute physicians or other medical staff, are medical devices (see question 2.6 for details). Where publicly owned hospitals purchase robotics, the transaction is subject to public procurement laws and a formal tender procedure must be regularly conducted.
- **Wearables**
  Wearables such as smartwatches often serve multiple purposes. Therefore, they are often not considered to be medical devices in their own right (see question 2.6 for details), but can be used with applications that qualify as medical devices (for instance an ECG application).
- **Virtual Assistants**
  A virtual assistant – e.g. Amazon's Alexa, Apple's Siri, or Microsoft's Cortana – is a software agent or device that is connected to the internet and can perform tasks or services for the user based on commands or questions. Such assistants are, *inter alia,* used in nursing care.
- **Mobile Apps**
  Mobile Apps may have a medical purpose and therefore can fall under the definition of a medical device (see question 2.6 for details). According to a recent modification in German Health Insurance Law, medical apps may – under certain conditions – be prescribed by physicians and reimbursed by public health insurers.
- **Software as a Medical Device (SaMD)**
  Please see question 2.6 for details.
- **AI-as-a-Service**
  AI is a self-learning and autonomously deciding software. AI can be a valuable assistant in medical decisions (see under question 8.1). In the case of AI-as-a-Service (AIaaS), a third party offers AI-based services, e.g. Microsoft (Azure) or IBM (Developer Cloud). Instead of buying specialised hardware or software, individuals and organisations can use AIaaS to save costs.
- **IoT and Connected Devices**
  The Internet of Things (IoT) connects physical objects and machines, *inter alia,* in the healthcare sector. The IoT includes smart devices and protocols for facilitating communication between these devices, as well as systems and methods for storing and analysing data collected by the connected devices.
- **Natural Language Processing**
  Natural Language Processing (NLP) describes techniques and methods for automatic analysis and representation of human speech. The purpose is the direct communication between humans and computers based on natural language (see also question 8.1). NLP may be one phase of text and data mining (TMT), the purpose of which is to detect new correlations in databases by means of algorithms. NLP is, *inter alia*, used in pharmaceutical research.

3.2 What are the key issues for digital platform providers?

Mobility and security are becoming steadily more important for platform services. Platform providers need to enhance the security of their platforms and mobile device management solutions. They need to take into account legal requirements (e.g. data protection, liability) and promote general trust (e.g. through user training).

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Personal data are primarily regulated by the EU General Data Protection Regulation (Regulation 2016/679/EU (GDPR)).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Under the GDPR, each data controller – i.e. the subject that determines the purpose and the means of the data processing (Art. 4 no. 7 GDPR) – is responsible for personal data being processed in compliance with all relevant data protection laws. In the context of digital health, there is generally more than one data controller, as more than one subject or entity determines – separately or jointly – the purpose and means of the data processing. Data controllers under the GDPR can include healthcare service provider(s), platform providers, and/or companies using a healthcare app for its services.

Pursuant to the GDPR and the additional relevant German data protection laws (e.g. the German Federal Code on Data Protection (BDSG)), health and patients' data belong to the special categories of personal data. Under Art. 9 para. 1 GDPR, the processing of special categories of personal data shall be prohibited, subject to the condition that the processing is justified by law, in particular Art. 9 para. 2 h) and g), para. 2 GDPR, or by the data subject's consent. Additionally, the patient's right to confidentially in the doctor-patient relationship, and the respective health-related data and other secret information are to be observed.

4.2 How do such considerations change depending on the nature of the entities involved?

Digital health affects more private subject and public entities than the traditional healthcare sector as, not only the patient, the healthcare provider and the regulating authorities are involved: with digital health, there are often third non-medical parties (e.g. the platform provider; or manufacturer of digital apps) rendering possible the use of digital health applications by services or products. The grounds that justify personal data processing by law, though, are generally limited to subjects that are bound by professional confidentiality obligations (e.g. physicians, nurses, healthcare insurers). Non-medical private stakeholders may principally process healthcare and patient data dependent on a prior and informed consent by the interested data subject. This requirement may create organisational difficulties, e.g. in case of databases or when huge amounts of health data are processed, as data subjects may withdraw their consent at any time.

4.3 Which key regulatory requirements apply?

In the context of digital health, the risk of data protection breaches and the severity of such breaches for rights and freedoms of natural persons may be high. Controllers have to assess the concrete risks once the appropriate technical and organisational measures are implemented and again when the personal data are processed (data protection by design and by default pursuant to Art. 25 GDPR).

The core activities of many private companies operating in the digital health sector consist of processing on large-scale health and patient data. In this case, the private company is obliged to designate a data protection officer responsible for all data protection issues (see Art. 37 para. 1 lit. c GDPR).

Furthermore, if the type of data processing is likely to result in a high risk to the rights and freedoms of a natural person, each controller – in particular if it uses new technologies like digital apps and other new electronic healthcare devices – shall carry out, prior to the commencement of processing, a data protection impact assessment. For a correct assessment, the controller shall take into account the nature, scope, context and purposes of the processing (Art. 35 para. 1 and para. 2 lit. c GDPR).

4.4 Do the regulations define the scope of data use?

Neither the GDPR nor the BDSG define the scope of data use in digital health.

Rather, the interested parties – the controller and affected data subject (e.g. app user) – decide about the scope of the data use in the concrete context. The contractual relationship, the used techniques, and the legal requirements and limits to process personal data under the GDPR (e.g. Art. 5 GDPR) influence how the parties determine the scope of the data use. Art. 5 lit. a and lit. b GDPR rules that personal data shall be collected and processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The permitted data processing is limited to the extent, which is adequate, relevant and necessary with regard to the agreed purpose. Due to these rules, the controller cannot agree with the data subjects to a "broad-brush" (blanket) scope for the data use. The controller must rather reveal as concretely as possible to the data subject the scope the personal data shall be used for, set up limits, and ask in this regard for specific consent. The data subject may give consent for one or more scopes of data use. If the controller intends to use the collected personal data for anything other than the agreed purpose, a new and/or additional consent from the data subject is required.

4.5 What are the key contractual considerations?

- Documentation:
  Data protection law generally does not rule any mandatory contractual form. Each data controller is obliged, however, to demonstrate that personal data are processed in compliance with all relevant laws within his business – e.g. the controller has to show that he processes personal data only to the extent of the agreed scope and based on the data subject's consent (or on another legitimate legal ground). Therefore, controllers shall document the key data of the data processing. Furthermore, from a healthcare law perspective, the service provider has to demonstrate that he gave all required information about the treatment of the patient and that the patient gave his/her explicit consent. Due to these documentation obligations, the controller shall enter into a written agreement with the data subject. The term "written" is to be interpreted with European principles and thus includes mail, e-mail and any other kind of permanent form. In the context of digital health, the exchange of written papers signed by the parties will rarely be used. Only some specific healthcare data provisions require this type of written consent by the data subject (patient), e.g. the German Code on Genetic Diagnostics (GenDG). Generally, explicit, but not necessarily hand-signed, consent from the data subject (patient) is sufficient.
- Joint Controllership Agreement:
  In digital health scenarios, there is often more than one data controller (see question 4.1). In such contexts, collaborating controllers must enter into an agreement on joint controllership pursuant to Art. 26 GDPR. The agreement under Art. 26 GDPR shall duly reflect the respective roles and relationships of the joint controllers towards the data subjects determining in a transparent manner their respective responsibilities under the GDPR and the related liability.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Data protection in the context of healthcare has a two-fold dimension.

The first dimension regards data protection under GDPR and national general data protection laws. General data protection laws focus on the data transfer between two or more individuals or legal entities. General data protection laws are not applicable within a legal entity, notwithstanding the fact that more than one natural person belongs to the legal entity and/or works there. The second dimension regards specific healthcare data protection laws (especially the principle of confidentiality between doctor and patient) that focuses on the allowed data transfer between individuals. Therefore, also within a company (e.g. a hospital) the requirements and limits ruled by these laws must be observed.

Both dimensions of data protection law must be cumulatively considered. The legal requirements may differ; in this case, specific healthcare data protection law is generally stricter and more limiting, e.g. personal data governed by the principle of confidentiality between doctor and patient may be transferred and processed only with the explicit consent of the patient.

5.2 How do such considerations change depending on the nature of the entities involved?

The obligation to keep confidential all personal data and information on patients binds physicians, pharmacists and other healthcare professionals, as well as personnel of assurance companies, including all their employees and assistants. All other natural and legal persons must comply with general data protection law only, subject to the condition they are not acting on behalf of a healthcare professional. In the latter case, non-medical persons are bound by the obligations of physician-patient confidentiality too.

Art. 9 para. 3 GDPR rules that the processing of special categories of personal data (e.g. healthcare data) can be justified by legal grounds only for professionals and other persons bound by confidentiality obligations. In all other cases, the person, company and/or entity must obtain a prior consent by the data subject to legitimately process healthcare data.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The requirements for sharing healthcare and other personal data between two different natural or legal persons are generally regulated by GDPR and the BDSG. Healthcare data may be additionally regulated by special laws, e.g. the GenDG.

Additionally, the principle of confidentiality between doctor and patient and other corresponding obligations are to be observed. The confidentiality obligation is governed by professional law. Breaches will be sanctioned by professional or, in severe cases, by criminal law.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patent protection is granted – by a patent office upon application only – for any invention having a technical character, provided that it is new, involves an "inventive step" and is suitable for industrial application. In digital health, the core technology (e.g. sensors and hardware) is generally patentable, even if patents remain mostly used in this rapidly developing environment. Accordingly, it is not surprising that the number of worldwide IoT patent applications increased substantially to over 130,000 in 2018 and the healthcare sector is contributing to this development.

6.2 What is the scope of copyright protection?

It is the idea of copyright law to grant exclusive, non-registered rights to the author or creator of the original non-technical work. This work can also take the form of a computer program, e.g. a statement, program language or mathematic algorithm, provided that it is an individual work and therefore the result of the author's own intellectual creation. However, efficient protection of an invention can only be achieved with the help of a patent; at most, copyright law can offer accompanying protection. Please note, however, that data created by digital health programs can never be subject to copyright because it is not an individual work and therefore not the result of an author's own intellectual creation.

6.3 What is the scope of trade secret protection?

Trade secrets can be an appropriate tool to generate value for digital health companies if patent protection is not available, e.g. regarding software source codes or algorithms. The prerequisite of trade secret protection is that it relates to something that can be kept secret and actually is kept secret through reasonable efforts. For example, obvious elements of technology (design, etc.) or business strategies, will not remain secretive once they are placed on the market. In order to actually keep secrecy, companies must – in accordance with the new German Secret Protection Act (GTSA) – implement a confidentiality program that includes organisational (e.g. trade secret policies), technical (e.g. IT security) and legal steps (e.g. extensive confidentiality clauses). Only the trade secret as such is protected, not the results achieved with it. This is relevant in the context of data protection, since, for example, a trade secret covering data processing means does not cover the generated data.

6.4 What are the typical results on academic technology transfer rules?

Academic technology transfer means the transfer of knowledge from its creator to another person or organisation by means of licence or purchase agreements. It is of great importance to the competitiveness of (small- and medium-sized) enterprises today.

Technology transfer agreements bear certain risks for the inventor, as the protection of secrets depends *de facto* on the counterparty's loyalty to the contract. Even a non-compete agreement cannot reverse a disclosure, when it happened. Besides, the licensee may act as a potential competitor and weaken the inventor's economic position.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

In the healthcare sector – as in other newly developed technical sectors – the main question is whether intellectual property protection is available for software inventions, e.g. SaMD.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

If medical software represents an abstract idea and therefore, protection is sought for computer programs "as such", there is no protection according to patent law. Under German and European patent law, protection is only possible for algorithms and methods underlying the programs that have an inventive step over the prior art – one that is found based only on features that contribute to the technical character. According to German case law, however, programs that immediately trigger a technical effect or directly optimise data processing hardware are considered patentable. The inventor(s) must always be human; "AI inventors" or "crowd inventors" do not exist. The same rules apply to copyright, since the underlying concept is never fully protected. Trade secret protection for SaMD is only possible under the restrictions described under question 6.3.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Collaborations between medical professionals, and collaborations between medical and non-medical professionals and companies, are generally permitted by law and can be very valuable in improving the quality of healthcare services. In particular, the sector of digital health services is a market with high potential for such innovative collaborations. Medical healthcare professionals are not allowed, however, to accept or request any payments or other favours in return for services, *inter alia*, for prescribing medication or medical devices or supplying patients or diagnostic data.

7.2 What considerations apply in agreements between health care and non-health care companies?

Only qualified professionals or legal entities – where medical services are managed by healthcare professionals – are entitled to provide healthcare services. In addition to the professional qualification, most healthcare professionals or legal entities require a permit, licence or contractual authorisation to be allowed to provide healthcare services. In consequence, non-healthcare companies can assist healthcare companies by providing non-medical services and goods to them or managing their business with regard to all non-medical issues. Regarding digital healthcare services, non-healthcare companies may be responsible, for example, for the technique, the payment procedure and/or additional provided services, like the transport to the hospital. They cannot provide, however, remote medical services in their own name or give orders to medical professionals on how to carry out their practice.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

It is common opinion that no other sector is more promising than healthcare when it comes to the question of whether humans benefit from machine learning. Machines that learn to recognise diseases in medical scans may offer better and faster treatment to patients. The value of this technical support increases if it also explains its decision, e.g. by highlighting the regions of the scans that are the reason for the diagnosis. It is conceivable – and sometimes already in existence – that machines learn to communicate with people and to take on individual tasks themselves, e.g. the administrative process in hospitals or the personalising of medical treatments.

Digital health devices and apps often depend on AI to work and improve. Please note, where a device is not fully developed, but subject to further development due to machine learning, this may constitute a hurdle to CE-marking.

8.2 How is training data licensed?

AI systems require vast amounts of training data to be effective. Licences can help close the gap if companies have incomplete, inaccurate, or not representative data. Training data is licensed according to the same rules as standard licensing. Thus, the creator/depositor of the data set and the user have to conclude a licence agreement, which specifies the licence conditions (e.g. attribution, copy-left, and non-commerciality), possible re-use rights and the licensing fee.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Under current law, only humans are capable of being inventors (see also question 6.5). There are suggestions to recognise an AI system as an inventor and the system's creator as the assignee or owner of its patents. Companies, however, are primarily interested in obtaining a patent; they pay less attention to the question of who the inventor is. Moreover, AI is to be defined as a tool as long as individuals instruct the AI and are the original source of the inventive capability. A minimum of human involvement is sufficient for the courts to identify this person as the inventor to whom the invention should belong.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Data can be a powerful tool for building new businesses. Against this background, licensing data seems to open up new revenue streams for companies. However, from a strategic point of view, such an approach could lead to undesired reinforcement of certain competitors. Moreover, in the future, machine-learning systems will require less and less data to learn sufficiently, which leads to predictable limits for a business model based on licensing data. In the end, companies will build their own data supply systems and until then, companies find a distinctive system of open-source offers in this area.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Special liability regimes related to digital health do not exist (yet) in Germany. Liability in this sector depends on the kind of healthcare services provided (e.g. remote medical treatment via video conference, remote monitoring of physical values or healthcare app use), the extent of direct involvement of healthcare professionals, and the kind of damages caused (e.g. physical harm, financial loss or intangible damage). Liability in digital health will be mostly qualified as contractual liability, and arise from torts. In addition, statutory liability might arise from law services (e.g. product liability, liability for physical harm and death).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

9.2 What cross-border considerations are there?

In case of cross-border digital health services, the interested parties have to determine the applicable national law. In some cases, the interested parties can decide on the applicable law, in others there is a mandatory applicable law; sometimes laws from more than one country may apply. If the digital healthcare services have an adverse outcome, the applicable liability regime will be established according to the rules of international private conflict law, which is based on objective criteria. Generally, the parties can only influence and decide on the forum of the proceedings.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Healthcare organisations that transfer IT operations to clouds in order to reduce cost and improve accessibility and management of patient data are facing legal, medical, technical, organisational, and economic challenges. Security and confidentiality are key aspects for a wide-scale use of cloud-based services. To reduce the risk of cyber-attacks and the loss of sensitive data, healthcare organisations must ensure a safe system to transfer, maintain and receive sensitive health information. Nevertheless, the interoperability between partners is to be guaranteed as well as a management system that enables multiple but secure access to relevant data, provides file synchronisation and shares services and alerts. Confidentiality can be achieved by access control and using encryption techniques. On the legal level, data protection requirements have to be observed, such as the obligation to exchange predominately anonymous or pseudonymised data.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Non-healthcare companies are not allowed to provide medical services to patients. Medical services are reserved to professionally trained personnel like physicians, other health professionals and private healthcare companies licensed for these services. Non-healthcare companies can support healthcare professionals providing them or their patients with auxiliary non-medical services. Non-healthcare companies may, however, distribute and sell medical devices like specific healthcare apps and other applications. This latter sector is not limited or reserved for specific healthcare professionals only.

The digital health sector is a quite new and complex market that is developing quickly. The current German Minister of Health, Jens Spahn, has started to address systematically the issue of reforming German healthcare laws, introducing and establishing step-by-step tele-medical services, including reimbursement of costs, in the standard medical care. This shows that the German digital health sector has not yet been fully regulated; today, there are only some specific laws and provisions ruling this sector. For non-healthcare companies this may be, on the one hand, an advantage because the digital healthcare market is open to new ideas and growth. On the other hand, the healthcare market is very sensitive (given the fundamental right to life and health) and conservative (the healthcare professionals in Germany have a strong lobby). This carries the risk that the German healthcare market does not develop as quickly as wished by companies and innovative thinking people. In the end, however, the innovation process has started and will hardly be impeded again.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

The outpatient medical healthcare sector is highly regulated – in particular for patients insured in the statutory healthcare system (around 90% of German residents). The permission to provide outpatient services to patients is limited to physicians and other licensed private companies (so-called medical care centres (MCCs)). Private persons or companies are not admitted as shareholders of MCC-companies. The position of private shareholder in a MCC-company is reserved, for example, to licensed physicians, providers of non-medical dialyse services and licensed hospitals.

If private digital health companies plan to operate in the outpatient sector, they should consider acquiring shares of a licensed hospital or a non-medical dialyse service provider, to collaborate with them or enter into joint ventures with public insurance funds or other competent public entities.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Dr. Stephan Rau focuses his practice on mergers and acquisitions (M&A) transactions and regulatory advice in the health and life science sector. He is the head of the Firm's Health Law Practice Group in Europe. In 2004, Stephan was an adviser on the foundation of the first German corporate medical centre. Since then, he has represented numerous investors, healthcare service providers, pharmaceutical and medtech companies, as well as governmental entities in M&A transactions, outsourcing projects, and licensing and reimbursement proceedings. Stephan speaks regularly at healthcare and life sciences industry conferences, as well as legal expert conferences, both at an international and national level. He is the author of numerous publications on German corporate law, healthcare and life sciences regulation.

McDermott Will & Emery LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 322
Email: srau@mwe.com
URL: www.mwe.com

Steffen Woitz – Partner, based in Munich – focuses his practice on litigation, intellectual property, antitrust and competition law and alternative dispute resolution. Steffen has in-depth litigation experience in all major German courts and assists clients in cross-border disputes and transactions. He represents German and international clients in patent infringement and other contentious matters relating to trademarks, unfair competition and antitrust law. In addition, Steffen is active in the area of cartel damages, having successfully defended clients against cartel damages claims brought by competitors and commercial customers. Steffen advises clients on cooperation and distribution agreements from a German civil law and an antitrust perspective. He has deep knowledge in the area of competition law compliance. He also advises on a broad range of intellectual property and antitrust issues in connection to national and international mergers & acquisitions.

McDermott Will & Emery LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 181
Email: swoitz@mwe.com
URL: www.mwe.com

Dr. Karolin Hiller – Counsel, based in Munich – specialises in the healthcare/life sciences sector, regulated industries and public commercial law. Karolin advises private companies and public corporations on regulatory and connected legal issues. Karolin is an experienced litigator who represents clients in social, administrative and civil proceedings at all judicial instances. Karolin focuses on statutory health insurance law, hospitals, telemedical healthcare services and nursing care. In the life science sector, she advises on medical device and (health) data protection law, including related compliance and litigation issues. Karolin is a member of the firm's legal cannabis industry group, a multidisciplinary and international team of lawyers providing clients with all legal services relevant for their investments in the cannabis industry.

McDermott Will & Emery LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 326
Email: khiller@mwe.com
URL: www.mwe.com

Jana Grieb specialises in healthcare and life sciences, with a particular focus on the pharmaceutical and medtech industry. Jana has advised numerous pharmaceutical and medical devices companies in a variety of regulatory issues, transactions and contractual matters across the European Union, with regard to product safety, public procurement law, unfair competition and reimbursement by public and private payers and has represented them in litigation and negotiations. Prior to joining McDermott, Jana worked for an international law firm and a Munich-based law firm focusing on pharmaceutical law.

McDermott Will & Emery LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 322
Email: jgrieb@mwe.com
URL: www.mwe.com

Our Life Sciences and Healthcare Industry Group provides a full spectrum of legal services required by private companies and public authorities, including representation in social, administrative and civil litigation.

Our life sciences attorneys conduct transactions in the pharmaceutical and medical device sector, advise on reimbursement of pharmaceuticals and give legal and strategic advice on all kind of medical issues. The team negotiate distribution and manufacturing agreements and advise in the context of compliance, advertising and product labelling.

Our attorneys are specialised in healthcare law structure and negotiate mergers and acquisitions for in- and out-patient medical services providers, and advise on laws relevant for healthcare insurance funds, hospitals and care homes and on general medical law including digital health issues.

They represent clients before health insurance organisations and admission boards, negotiate all kinds of healthcare contracts and offer legal advice in matters of public procurement law. They also support companies and start-ups in the field of cannabis for medical use.

www.mwe.com

McDermott Will & Emery
RECHTSANWÄLTE STEUERBERATER LLP

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Greece


Irene Kyriakides


Dr. Victoria Mertikopoulou

Kyriakides Georgopoulos Law Firm

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

The Greek Ministry of Health uses the European Commission's definition of digital health, according to which "*Digital health and care refers to tools and services that use information and communication technologies (ICTs) to improve prevention, diagnosis, treatment, monitoring and management of health and lifestyle*" (see also Communication on Enabling the Digital Transformation of Health and Care in the Digital Single Market), as well as the definition of eHealth provided by the WHO, according to which "*eHealth refers to the use of information and communications technology in support of health and health-related fields*".

1.2 What are the key emerging technologies in this area?

The key emerging technologies in health may be divided into the following main categories:

- Artificial intelligence and its applications in the health sector.
- Robotic medicine.
- E-health and users' protection/telemedicine/wearable devices/remote diagnostic and monitoring systems/cloud-based integration of medical devices.
- Emerging medical therapeutic technologies.
- Big data analytics.
- Virtual and augmented reality.
- Genomics.

It is noted that in the near future, electronic cross-border health services are progressively being established in Greece (namely in order to accept/make available ePrescriptions and Patient Summaries originating from another European country (digital access to ePrescriptions and Patient Summaries)).

On a national level, patients shall be able to receive information on their medical treatment and medicine renewal *via* SMS, and physicians will be able to issue electronic prescriptions, without the patients' physical presence being required. The set-up for e-Prescriptions is scheduled to be operational by the end of March 2020. Moreover, a bill for e-ΕΦΚΑ is currently under consultation (until 7 February 2020), providing for medical certificates to be issued *via* the Electronic Prescription System of IDIKA AE (ΗΔΙΚΑ ΑΕ/e-Government Center for Social Security Services).

Currently, a national framework for the interoperability of health systems has been set up. The "112" European emergency phone number is in place. Moreover, it is worth noting that the introduction of a single identification number for all citizens is under way, and this number shall be introduced in all technology systems including health and social security within a two-year timeframe.

1.3 What are the core legal issues in health care IT?

Due to the digitalisation of healthcare systems and the maintenance of electronic records with medical data, there is a need to protect that sensitive information from any unauthorised release. Hence, the core legal issues of healthcare IT may be categorised as follows:

- Patients' privacy/data safety/data security.
- Cybersecurity.
- AI-related and other healthcare IT ethical issues.
- Reliability of automated diagnoses.
- Doctor-patient relation/eSkills for professionals.
- Interoperability.

The issue of medical regulatory submission requirements often arises.

2 Regulatory

2.1 What are the core health care regulatory schemes?

Legal provisions relating to healthcare may be found in a number of legislative acts and regulations, the most important of which are the following:

- Legislative Decree 96/1973 on the trading of pharmaceutical and cosmetic products.
- Law 1316/1983 on the establishment, organisation and competence of the National Organisation of Medicines, the National Pharmaceutical Industry, the State Pharmaceutical Warehouse and other provisions.
- Law 1965/1991 which amended the abovementioned Law.
- Ministerial Decision Y6a/22261/2002 on the advertisement of pharmaceutical products that may be administered without prescription.
- Ministerial Decision DY8d/G.P.oik.130648/2009 on medical devices.
- Ministerial Decision DYC3a/32221/29.4.2013 on the implementation of the Directive 2001/83/EC of the European Parliament and of the Council on the Community Code relating to pharmaceutical products for human use.
- Ministerial Decision G5a/59676/2016 on clinical trials (transposition of Regulation 536/2014).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- Ministerial Decision oik15779/D.T.B.N 266/2016 transposing the Directives 2015/573/EU and 2015/574/EU.
- Ministerial Decision A3(g)/G.P./oik 25132/2016 on access for uninsured people to the Public Healthcare System.
- Law 4486/2017 that amended the previous legislation (namely Law 4238/2014) on the National Primary Health Care Network (PEDY), on the change of scope of the Greek National Health Service (EOPYY) and other provisions.
- Law 4529/2018 articles 22–23 on social security.
- Law 4600/2019 and Law 4633/2019 (establishing the National Public Health Organisation) aiming for a general modernisation of Greek healthcare.
- Various circulars of the National Organisation for Medicines (EOF).
- The Hellenic Association of Pharmaceutical Companies (SFEE) Code of Ethics (provisions of said Code are binding only for the members of SFEE).

2.2 What other regulatory schemes apply to digital health and health care IT?

Greek legislators provided the following series of legislative provisions that specifically address digital health and healthcare IT:

- Law 3984/2011 article 66 par. 16 on telemedicine.
- Ministerial Decision A5(d)/G.P.oik 85140/2015 regulating the operation and the responsibilities of the National Council for eHealth Governance.
- The Presidential Decree 121/2017 on the structure and responsibilities of the eGovernment Divisions, regulating the responsibilities of the Department of Health Data Management.
- Law 4600/2019 article 84 regulating the individual patient's medical file.
- Law 4624/2019 transposing the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data.
- Presidential Decree 81/2019 establishing the Hellenic Ministry of Digital Governance.
- Ministerial Decision A3(d)/G.P.oik. 15332/2019 on the establishment of the National Council for eHealth Governance.

2.3 What regulatory schemes apply to consumer devices in particular?

The main national regulatory schemes that apply to consumer devices are as follows:

- Law 2251/1994 on consumers' protection as amended by Law 3587/2007 and Law 4512/2018 articles 100 *et seq*.
- Ministerial Decision Z3/2810/2004 transposing the Directive 2001/95/EC on general product safety.
- Law 4177/2013 on regulating the market of products and the provision of services.
- Ministerial Decision 5338/2018 that codifies the provisions of Law 2251/1994.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The main Greek regulatory authorities are:

- The Hellenic Ministry of Health (https://www.moh.gov.gr/articles/ehealth) is responsible for protecting and promoting the public's health through planning and implementing Public Health policies, and ensuring universal and equal access to healthcare services provided by the National Health System, as well as regulating the operation and supervision of private healthcare providers. In particular, the Ministry of Health shall:
  (a) recommend measures to the government;
  (b) inform the members of the Hellenic Parliament;
  (c) represent Greece in the European Union, in third countries, in international organisations, etc.; and
  (d) cooperate with other ministries, public services and organisations.
- Regulation and supervision of pharmaceutical products and medical devices is effected ultimately by the Ministry of Health, which is responsible for the Greek pharmaceutical policy, and the *National Organisation for Medicines* (EOF) (https://www.eof.gr/web/guest;jsessionid=0bd2dc582d-d4612032a240b679d7) which is the national authority for the regulation and surveillance of the research, manufacturing, marketing and commercialisation of pharmaceutical products, medical devices and others (e.g. cosmetics, food supplements and veterinary products, homeopathic medicines, herbal products, vitamins, biological products and minerals).
- The National Transparency Authority, bringing together six separate supervisory agencies among which is the Inspectors-Controllers Body for Public Administration.
- The Hellenic Ministry of Digital Governance, responsible for regulating Cyber Security as well as Telecommunication.
- The Hellenic Data Protection Authority (HDPA), whose purpose is to secure the protection of natural persons with regard to the processing of personal data and the free movement of such data by issuing guidelines and/or decisions in cases of violation.
- The National Council for eHealth Governance, whose purpose is to provide consulting and advising services to the Hellenic Ministry of Health and recommending policy priorities, action plans and necessary institutional reforms.
- The National Cyber Security Authority, responsible for the security of network and information systems, safeguarding the compliance with the relevant regulatory framework.

Moreover, the following bodies should be mentioned:

- The Council for Monitoring Communication (Greek acronym: SEE) is an independent, non-profit civil association which monitors the content of advertising messages before their transmission by electronic media and examines their accordance with the relevant legislation and the SEE's Code of Ethics.
- Furthermore, the Hellenic Association of Pharmaceutical Companies (Greek acronym: SFEE) – member of the European Federation of Pharmaceutical Industries and Associations, and the Association of Health-Research & Biotechnology Industry (Greek acronym: SEIV), also monitor the compliance of pharmaceutical products and medical devices advertisements with their Codes of Ethics, mandatory for their members, thus imposing additional sanctions in case of infringements.
- Association of Pharmaceutical Companies for Products of OTC medicines (http://www.efex.gr/).
- The National Computer Security Incident Response Team, whose main responsibilities are: (a) monitoring relevant incidents at national level; (b) providing timely warnings, alerts and notifications; (c) intervening in case of an incident; (d) providing a dynamic risk and incident analysis as well as awareness of the situation; (e) participating in the CSIRT network and cooperating with the corresponding services of the other Member States; and (f) promoting, adopting and using standard international and European practices.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The regulations falling under the competence of the Hellenic Ministry of Health and the Hellenic Ministry of Digital Governance constitute the key areas of enforcement; their implementation is monitored and infringements are sanctioned by Greek enforcement bodies and Greek courts.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

According to European and national legislative provisions, software may be considered as a medical device under certain conditions (see also non-binding Guidelines on the Qualification and Classification of Stand-Alone Software Used in Healthcare within the Regulatory Framework of Medical Devices). The relevant regulatory texts on medical devices (i.e. Directive 93/42/EEC, Directive 98/79/EC, Regulation (EU) 2017/745) are applicable in all Member States. Under Greek legislation, Ministerial Decision DY8d/G.P.oik.130648/2009 on Medical Devices, regarding the transposition of "Council Directive 93/42/EEC of 14 June 1993, concerning medical devices", as amended, determines the legal framework and the definition of software as a medical device. In article 1, it refers to any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of (a) diagnosis, prevention, monitoring, treatment or alleviation of disease, (b) diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, (c) investigation, replacement or modification of the anatomy or of a physiological process, and/or (d) control of conception. It is noted that on 26 May 2020, the provisions of the Regulation (EU) 2017/745 shall also come in force.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Even though telemedicine is provided in law 3984/2011, stipulating that telemedicine services are provided if possible and under the responsibility of the treating physician dealing with the particular incident, a National Telemedicine Network was developed in 2016 by OTE Group on behalf of the 2nd Regional Healthcare Administration of Piraeus and the Aegean. So far 43 telemedicine units have been installed in 30 health centres on islands, 12 in regional and central hospitals and one in the main facilities of the Hellenic Ministry of Health. However, the absence of an extensive legal framework on telehealth raises concerns about medical liability, data safety and security, funding, as well as about the lack of the required telemedicine infrastructure in the remotest regions of the country. Private telecommunication companies try to address the latter problem by developing their own telemedicine programmes, providing thus access to healthcare professionals and health centres in areas that are not covered, or at least sufficiently, by the National Telemedicine Network.
- **Robotics**
  Although robotics is commonly used in the medical sector, mainly for surgical or patient-supporting purposes, there is no regulation specifically regarding robotics. On the basis of Directive 93/42/EEC and on the criteria and the definition provided by the Resolution on "European Civil Law Rules in Robotics", robotically assisted surgical (RAS) devices are classified as medical devices of class IIb and are therefore regulated in Greece under Ministerial Decision DY8d/G.P.oik.130648/2009.
- **Wearables**
  The core concern with wearable devices is their classification. Depending on their purpose, they may or may not be subject to the Ministerial Decision DY8d/G.P.oik.130648/2009 on medical devices. More specifically, wearable technologies should be divided into medical data collectors and wellness data collectors, according to the type of information they are programmed to record. Hence, wearable sensors that collect information on vital and/or biochemical signs for diagnostic, monitoring or predicting purposes may be classified as medical devices themselves, or as an accessory used along with a medical device. However, sensors that record and collect information only for self-tracking purposes are not regulated under the aforementioned Ministerial Decision, as they only resemble the operation of medical devices, and their purpose is to collect data on wellness signs such as calories, rather than diagnostic or disease monitoring data.
- **Virtual Assistants (e.g. Alexa)**
  Taking into consideration that virtual assistants are not yet incorporated into the Hellenic healthcare system, and health information from the NHS is not available through voice-assisted technology, there are no further identifiable issues other than the ones provided by European bibliographic references.
- **Mobile Apps**
  The main issue concerning mobile applications is the fact that, depending on their classification, different regulatory schemes may be applicable. Mobile apps should be divided into the following categories: a) health apps; b) medical apps; c) apps for the public; and d) apps for healthcare professionals. In particular, health apps, including fitness apps, have to be distinguished from medical apps as their purpose is to record wellness data and/or propose tutorials on healthy daily habits; whereas, medical apps have a more patient-centered perspective, monitoring and/or managing chronic diseases, recording vital and/or biochemical signs, reminding and/or recording medication, etc. Medical apps may be further classified into apps designed to be used by the general public *versus* apps designed for healthcare professionals. The latter apps may include electronic prescription, medical products dosage guidance, medical calculators, clinical guidelines, textbooks, literature search portals, health records, *et al.* However, Ministerial Decision DY8d/G.P.oik. 130648/2009 on medical devices is only applicable to medical apps that (a) can be classified as an accessory of medical devices recording and maintaining medical data, (b) transform the smart device into a medical device by attaching additional sensors, and/or (c) constitute an integrated medical software system providing personalised diagnoses to support the clinical decision-making. Therefore, other types of apps have to be regulated under different regulatory schemes depending on the provided services.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- **Software as a Medical Device**
  Software malfunction is a main concern as it may cause loss of sensitive medical data, which can be important and/or vital for diagnostic, monitoring, predicting or treating purposes, thus jeopardising the patient's health. Additionally, another key concern consists of ensuring data confidentiality, integrity and availability.
- **AI-as-a-Service**
  To this day, no European or national legislation on AI is in place. A high-level expert group on AI has been established and has issued "Ethics guidelines for trustworthy AI". MedTech Europe released a position paper on 28 November 2019, with the purpose of outlining the potential of AI in healthcare, as well as to recommend specific policies that could help establish a comprehensive common EU legal framework.
- **IoT and Connected Devices**
  The Internet of Things (IoT) raises challenges in respect of the data's management and storage. First of all, as the connected devices are of different categories (e.g. wearable sensors, mobile apps), the collected data is of heterogeneous formats. Hence, the connected devices may not interpret the data in the same way, thus possibly losing important medical information. Additionally, another concern is data quality, as the extracted information is of different quality and the connected devices do not have an evaluation system. Last but not least, the methods of transferring data (e.g. Bluetooth, Cloud services) are vulnerable to hacking and/or malfunctions, potentially releasing sensitive personal data and thus infringing national and/or European data legislation. Therefore, the development of a platform that addresses the above concerns is of paramount importance.
- **Natural Language Processing**
  On the basis that natural language processing is considered a branch of AI, the abovementioned comments on AI are also applicable in this section. There is no specific legislation in Greece.

3.2 What are the key issues for digital platform providers?

Digital platforms are subject to many applicable regulatory schemes such as data protection law, competition law and consumer protection law, as well as the EU regulatory framework on digital platforms. Hence, the relevant legal framework is very broad and therefore complex. Additionally, the key issues arising from digital platforms are: data security and lawfulness of processing; determining the appropriate retention period for each category of data; adducing appropriate safeguards in case of cross-border data transfers; and protecting patients' sensitive data – in short, data safety/data security issues.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The Greek legislation on personal data, Law 4624/2019, aims to complement the GDPR provisions. According to article 5 of Law 4624/2019, the main consideration on the use of personal data is to identify the correct legal basis on which processing is based, as well as to ensure that the processing purpose pursued is compatible with Greek law. Furthermore, it is imperative that the other main principles established by article 5 of the GDPR are also adhered to, particularly the principle of data integrity and confidentiality.

4.2 How do such considerations change depending on the nature of the entities involved?

The abovementioned considerations do not change depending on the nature of the entities.

4.3 Which key regulatory requirements apply?

The key regulatory requirements when processing special categories of data under article 22 of the Law 4624/2019 are:

- The signing of a data processing agreement.
- The respect of all the technical and organisational requirements of GDPR.
- Measures to ensure the ex-post verification and determination of data breaches.
- Measures to raise awareness of people responsible for processing data.
- Establishing access rights within the organisation of the controller/processor.
- Implementing the necessary security measures such as pseudonymisation of personal data and encryption of personal data in order to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- Establishing procedures to evaluate the effectiveness of the adopted technical and organisational measures ensuring the safety of processing.
- The appointment of a Data Protection Officer (DPO).

4.4 Do the regulations define the scope of data use?

Other than the GDPR, according to article 22 of the Law 4624/2019, data processing/use by private entities and/or public authorities are allowed, if it is required for: (a) social security and social protection reasons; (b) preventive medicine, the evaluation of employees' ability to work, medical diagnosis, health or social care or health or social care systems and services, or any agreement with a healthcare professional that has to respect professional secrecy; and (c) public policy reasons. Additionally, Greek legislators specified the abovementioned provision (c), regulating the necessity of data processing/use in cases of public interest, significant threat to national security or public security and humanitarian measures.

4.5 What are the key contractual considerations?

There are no specific provisions in Law 4624/2019 with regard to this matter. Under the GDPR it is essential to identify the role of the parties involved, as processors are controllers, so as to include in the contract the adequate contractual clauses, as well as to provide appropriate safeguards as required by the GDPR, in case personal data is transferred to data recipients/processors located in third countries.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The main considerations on data sharing are the same as those mentioned in question 4.1.

5.2 How do such considerations change depending on the nature of the entities involved?

The abovementioned considerations do not change depending on the nature of the entities.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The aforementioned requirements in question 4.3 on data use/processing are also applicable to data sharing. According to article 26 of Law 4624/2019, the transfer of personal data between public authorities shall be permitted only when it is necessary for the performance of the duties of the transmitting body or of the third party to whom the data is transmitted. However, the provision establishes further requirements in case the transfer is conducted from a public authority to private bodies, namely (a) the transfer has to be necessary for the performance of the duties of the transmitting body, (b) the third party to whom data is transmitted has a legal interest in the transmission and the data subject has no legitimate interest in not transmitting the related data, and (c) processing is necessary for establishing, exercising or supporting legal claims.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patents are protected on the basis of the provisions and conditions set by Law 1773/1987 as amended and in force. Said law ensures that the beneficiary of the patent is granted absolute protection, and this constitutes an important motivation for developing inventions. Moreover, the said legislation expressly defines the requirements and the process to be followed in order for the patent to be awarded, determines the respective criteria on the priority of patent applications, and also regulates its transfer, license, declaration of invalidity and revocation. Last but not least, this legislation provides for the establishment and functions of the Industrial Property Organisation, granting the latter with fundamental competencies.

6.2 What is the scope of copyright protection?

Copyright protection is regulated by Law 2121/1993, as amended and in force. It provides the definition of intellectual property works, determines both the proprietary and ethical character of the right granted to the creators' works, provides for related rights, ensures that the creator maintains their personal association to his/her work, permits licensing for use, promotes the economic exploitation of the work while at the same time it establishes a legal framework incorporating all relative EU Directives. Further, on 13 December 2017, the Greek Parliament adopted Law 4481/2017 giving emphasis on regulations of collective management of intellectual property rights. For the cases not specified in the aforementioned legislation, the Greek Civil Code is applicable.

6.3 What is the scope of trade secret protection?

Directive (EU) 2016/943 of the European Parliament and of the Council regulates the issue of the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. The said Directive was transposed into the Greek legal system on 1 April 2019 by virtue of Law 4605/2019, with article 1 thereof containing legislative definitions and provisions adopted by the EU Directive.

6.4 What are the typical results on academic technology transfer rules?

Law 1733/1987, articles 21, 22, Law 2741/1999, article 23 and Law 4310/2014 regulate academic technology transfer in Greece. The above laws apply to technology transfer contracts, filing of technology transfer contracts, licensing, support and institutional issues. Not all the necessary administrative acts on regional level have been issued and there is an issue of competencies at national and regional levels.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Software as a Medical Device is protected by the Intellectual Property Law 2121/1993.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The following considerations apply to collaborative improvements:

- Legal considerations (competition, data transfer, data use).
- Commercial considerations:
  - Need for organisational strategies.
  - Differentiated cultural backgrounds.
  - Limited survey results.
  - Leadership issues.
  - Interdisciplinary approach.

7.2 What considerations apply in agreements between health care and non-health care companies?

Depending on the nature and the objective of the agreement between healthcare and non-healthcare companies, the following considerations may apply:

- Competition rules.
- Intellectual Property rights.
- Confidentiality.
- Personal data protection.
- Special applicable regulations on medical devices (e.g. authorisations by competent authorities).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

The digital healthcare industry is being rapidly transformed by the clinical use of machine learning algorithms. Machine learning and AI technologies in general have recently been penetrating all areas of healthcare services, from improving digital healthcare management to new drug discovery. Algorithms will be implemented in the clinical setting of the healthcare professionals by embedding them in smart devices through the Internet of Things and could also be used by patients for managing chronic conditions of diseases.

In particular, machine learning applies to the following fields:

- Disease identification/diagnosis.
- Personalised treatment.
- Treatment and prediction of disease.
- Smart records.
- Medical data.
- Drug discovery and manufacturing.

8.2 How is training data licensed?

Training data is a certain percentage of an overall dataset along with the testing set which are used in order to train an algorithm. Protected works are often used in the training data sets. Those protected works are then enhanced by others by adding things like bounding boxes and labels. It is unclear what rights exist in these data sets because this is not yet a regulated area.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

This area has not yet been regulated. The parties involved should regulate the relevant issues in their commercial agreements to fill the gaps in the regulatory framework.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Licensing data is key to developing new AI and ML systems. Commercial considerations relate, *inter alia*, to accessing and securing quality data with the least restrictions possible. This entails negotiations with third parties and regulators and requires emphasis on the creation and management of data retention and usage policies. Attorneys work with the development team in order to fully assess design choices and ensure compliance with regulatory/privacy legislation.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Product liability is considered in the sense of allocation of liability in a complex chain of liability for a product or a component causing injury to an individual, taking into account the likely event of transfer of protected health information. This chain may involve the medical device company, eventually an application, cloud storage, the product manufacturer, data breaches, a cybersecurity event, the software developer, the healthcare provider, and wireless networks.

9.2 What cross-border considerations are there?

The main cross-border considerations are:

- Jurisdictional issues under Private International Law (Greek Civil Code articles 4–33).
- Patients' rights.
- Exchange of health data (GDPR).

10 General

10.1 What are the key issues in Cloud-based services for digital health?

The key issues in cloud-based services are:

- Cybersecurity – technical safeguards.
- Data transfer.
- Data use.
- Data protection.
- Intellectual property rights.
- Interoperability.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

The key issues that a non-healthcare company should consider are:

- The special applicable regulatory framework on medical devices (e.g. authorisations by competent authorities).
- Intellectual Property rights.
- Radical changes in the relevant market due to technological developments.
- Competition from different types of business models (large corporations and start-ups).
- Innovation.
- Specialised and interdisciplinary educated manpower.
- The fact that Greece's digital healthcare is not quite developed yet.
- To tailor a business plan specialised to the healthcare industry because of the way that it is structured and because of consumer expectations.
- Cultural differences.
- Developing a data strategy.
- Developing a corporate compliance plan.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

The key issues that venture capital and private equity firms should consider are:

- Funding options (loans, state aid).
- Greece's complex tax legislation.
- Bureaucracy.
- Grey areas on regulatory framework – accepting taking risks.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Irene Kyriakides heads KG's Life Sciences/Pharmaceutical Practice Group as well as the Intellectual Property Practice Group. She has particular experience in all matters related, amongst others, to medicinal products, medical devices, cosmetics, food supplements and veterinary products and has successfully handled complex projects in the pharma sector. Irene advises major pharmaceutical companies in their day-to-day operations including routine healthcare contracts, compliance programs and regulatory issues. Irene's experience in the area of IP regulation and legislation enables her to offer full professional services and support on both contentious and non-contentious issues covering the standard areas of IP such as trademarks, copyrights, patents and domain names. Irene undertakes the filing of oppositions, cancellations and recourses, representing clients before the Trademarks Committee and the Administrative Courts.

Kyriakides Georgopoulos Law Firm
28 Dimitriou Soutsou Str.
GR 115 21
Athens
Greece

Tel: +30 210 817 1591
Email: i.kyriakides@kglawfirm.gr
URL: www.kglawfirm.gr

Dr. Victoria Mertikopoulou is Counsel, EU & Competition, Regulatory and Compliance. Her practice focuses on EU law, competition/dominance, horizontal and vertical agreements and distribution, regulatory and compliance, digital economy and consumer protection, dawn raids, and procedural issues before administrative authorities. Prior to joining KG Law Firm, Victoria served as a member of the Directorate General of Competition and, since 2012, as Commissioner – Rapporteur, Member of the Board of the Hellenic Competition Commission. She is a member of the Athens' Bar Association and holds a Ph.D. in EU Competition Law from the University of Athens and an LL.M. in International Business Law from the University College London (UCL). Previously, she worked as a lawyer, advising on matters of EU competition and commercial law, and as a stagiaire at the European Court of Justice. Victoria has substantial experience from her participation in European and International organisations (*inter alia,* ECN, OECD, and ICN). She has authored many articles for leading industry publications and has given lectures at conferences and universities on her areas of expertise. She was selected as one of the top Notable Women Competition Professionals in Europe, the Americas and Africa (Enforcement, Judiciary and Policy) by the W@Competition selection board.

Kyriakides Georgopoulos Law Firm
28 Dimitriou Soutsou Str.
GR 115 21
Athens
Greece

Tel: +30 210 817 1545
Email: v.mertikopoulou@kglawfirm.gr
URL: www.kglawfirm.gr

KG Law Firm retains a strong Life Sciences & Healthcare Practice, as reflected in the growth path of the firm over the years, active in the pharmaceutical and medical devices sectors, but also covering cosmetics, food supplements, food for special (medical) purposes, veterinary products and other highly regulated products. Our track record includes key transactions and projects, while the team operates across multiple practice groups in an open, flexible manner, to thus offer our clients integrated and cost-effective solutions on all related issues. On a general note, clients turn to our Life Sciences team in order to obtain timely and cost-efficient advice to a full range of regulatory, compliance and legal concerns. Our longstanding work in the life sciences regulatory environment makes us uniquely familiar with the latest issues and challenges that the industry faces. This deep understanding – also informed by our work done for manufacturers, importers, investors and many other players in the healthcare industry – allows us to promptly recognise and resolve new and old issues alike. That, in turn, allows us to advise clients on how best to optimise their business and implement those models while avoiding pitfalls.

www.kglawfirm.gr

KG
KYRIAKIDES GEORGOPOULOS
Law Firm

© Published and reproduced with kind permission by Global Legal Group Ltd, London

India


Rajeev Kumar


Pankaj Musyuni

LexOrbis

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

In general, digital health in India refers to the tools and services used for health services with the help of information and communication technologies, including the prevention, diagnosis, treatment, monitoring and management of diseases. The Ministry of Health and Family Welfare (MoHFW) regulates this sector.

1.2 What are the key emerging technologies in this area?

The digital health sector is continuously growing in India and some of the key emerging technologies include: telemedicine; the Internet of Medical Things (IoMT); robot-assisted surgery; self-monitoring healthcare devices; Electronic Health Records (EHR); Health Service Aggregation; mobile health; targeted advertising; e-pharmacies; cloud computing; and Artificial Intelligence (AI).

1.3 What are the core legal issues in health care IT?

As there is a regular exchange of information regarding health issues between the patient and the service provider, personal data protection is of prime concern. Although the Information Technology Act, 2000; Data Protection Rules, 2011; and Intermediaries Guidelines, 2011 are available, no standards have yet been set to mandate the implementation of data protection and security. Recently, the Personal Data Protection Bill, 2019 was introduced in Lok Sabha, on 11 December 2019. The said Bill seeks to provide for the protection of individuals' personal data and establishes a Data Protection Authority for the same.

2 Regulatory

2.1 What are the core health care regulatory schemes?

Healthcare schemes in India can be broadly classified under Central Sector Schemes, Centrally Sponsored Schemes and State Schemes. At national level, the Ministry of Health and Family Welfare (MoHFW) is the supreme body. Further, at state level, the organisation is under the department of health and family welfare of each state which is headed by a minister and has a secretariat under the charge of the Secretary or Commissioner (Health and Family Welfare) belonging to the cadre of the Indian Administrative Service (IAS). In addition, at regional level, each regional and zonal set-up covers three to five districts and acts under authority delegated by the State Directorate of Health Services; at district-level, the structure of health services is a middle-level management organisation that provides a link between the state and the regional structures on one side, and the primary health centres and sub-centres on the other. Furthermore, at community level, one community health centre has been established which provides basic specialty services in general medicine, paediatrics, surgery, obstetrics and gynaecology. Various schemes such as: Pradhan Mantri Swasthya Suraksha Yojana; the National AIDS and STD Control Programme; Family Welfare Schemes; the National Pharmacovigilance Programme; National Organ Transplant Programme; Impacting Research Innovation and Technology (IMPRINT) Scheme; and Swachhta Action Plan (SAP) are covered under Central Sector Schemes. Further, programmes such as the National Health Mission (NHM), National Rural Health Mission (NRHM) and National Urban Health Mission (NUHM) are centrally sponsored schemes which cover various other sub-schemes.

2.2 What other regulatory schemes apply to digital health and health care IT?

Some of the key ongoing initiatives in digital health being implemented by MoHFW include: Reproductive Child Healthcare (RCH); Integrated Disease Surveillance Program (IDSP); Integrated Health Information System (IHIP); e-Hospital, e-Shushrut, Electronic Vaccine Intelligence Network (eVIN); Central Government Health Scheme (CGHS); Integrated Health Information Platform (IHIP); National Health Portal (NHP); National Identification Number (NIN); Online Registration System (ORS); Mera Aspatal (Patient Feedback System); Health Management Information System (HMIS); and National Medical College Network (NMCN). These initiatives are operational at a substantially mature level and are already generating an enormous amount of data in the health sector. Since health is a state subject, states are supported under the National Health Mission (NHM) for services like Telemedicine, Tele-Radiology, Tele-Oncology, Tele-Ophthalmology and Hospital Information System (HIS).

2.3 What regulatory schemes apply to consumer devices in particular?

Consumer devices are usually protected under the Designs Act, 2000. A 'design' has been defined to mean only features

© Published and reproduced with kind permission by Global Legal Group Ltd, London

of shapes, configurations, patterns, ornaments or the composition of lines or colours that are applied to an 'article'. In terms of digital health, the two major components that would require design protection would be the Graphical User Interface (GUI) of applications and the design of the devices. GUI may be protected under the Designs Act, more specifically under Article 14-04 of the Design Rules, 2001, which covers 'Screen Displays and Icons'.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The Central Drug Standards Control Organisation (CDSCO) is the prime regulatory authority which looks into provisions of The Drugs and Cosmetics Act, 1940 and Rules thereof. Further, the practice of medicine is regulated by the Medical Council of India. In addition, the protection in terms of intellectual property is regulated under the Office of the Controller General of Patents, Designs and Trade Marks (CGPTDM) and copyright is governed by the Copyright Office, both under the Department for Promotion of Industry and Internal Trade (DPIIT).

The legal and regulatory framework is usually governed by following relevant Acts:

1. The Information Technology Act, 2000, The Information Technology (reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 and the Information Technology Rules, 2011.
2. Other Service Providers Regulations under the New Telecom Policy 1999.
3. The Drugs and Cosmetics Act, 1940 and Drugs and Cosmetics Rules, 1945.
4. The Indian Medical Council Act, 1956 and The Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002.
5. The Drugs and Magic Remedies Act, 1954 and Drugs and Magic Remedies Rules, 1955.
6. Unsolicited Commercial Communications Regulations, 2007 and Telecom Commercial Communication Customer Preference Regulations, 2010.
7. The Clinical Establishments Act, 2010.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

Key areas for enforcement include standards and ensuring security, confidentiality and privacy of patient's health and records.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

The Central Drug Standards Control Organization (CDSCO) under Directorate General of Health Services (Ministry of Health & Family Welfare) is the primarily responsible authority for regulating medical devices and diagnostics in India. **The Drug Controller General of India** (DCGI) is the key official within the CDSCO. The DCGI is responsible for the approval of the manufacturing of certain drugs (vaccines, large volume parenterals, blood products, r-DNA derived products), specific medical devices, and new drugs. In India, the manufacturing, import, sale, and distribution of medical devices are regulated under **India's Drugs & Cosmetic Act and Rules** (DCA).

In India, at present only notified medical devices are regulated as 'drugs' under the Drugs and Cosmetics Act 1940 and Rules made thereunder in 1945:

1. (i) substances used for *in vitro* diagnosis and surgical dressings, surgical bandages, surgical staples, surgical sutures, ligatures, blood and blood component collection bag with or without anticoagulant covered under sub-clause (i);
2. (ii) substances including mechanical contraceptives (condoms, intrauterine devices, tubal rings), disinfectants and insecticides notified under sub-clause (ii); and
3. devices notified from time to time under sub-clause (iv), of clause (b) of Section 3 of the Drugs and Cosmetics Act, 1940.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  - A. System development, maintenance and implementation cost.
  - B. Digital awareness and technology acceptance.
  - C. Diagnostic accuracy.
- **Robotics**
  - A. Energy storage.
  - B. Ethics and security.
- **Wearables**
  - A. Cost of device.
  - B. Battery life.
  - C. Safety, security and privacy.
- **Virtual Assistants (e.g. Alexa)**
  - A. Lack of accuracy.
  - B. Lack of analytical interpretation.
- **Mobile Apps**
  - A. Competitive market.
  - B. Promotion and marketing.
- **Software as a Medical Device**
  - A. Software development lifecycle.
  - B. Product safety and security.
  - C. Data collection and privacy.
- **AI-as-a-Service**
  - A. Reliance.
  - B. Transparency and governance.
  - C. Long-term cost.
- **IoT and Connected Devices**
  - A. Compatibility of operating systems.
  - B. Identification and authentication of devices and technologies.
  - C. Integration of IoT products and platforms.
  - D. Connectivity.
  - E. Data analytics, security and privacy.
  - F. Consumer awareness.
- **Natural Language Processing**
  - A. Understanding of natural language.
  - B. Reasoning about multiple documents.
  - C. Identification of data and evaluation of problem.

3.2 What are the key issues for digital platform providers?

The primary issues for platform providers stem from the transitional phase of adopting new technologies. Accordingly, the following issues are of primary concern for digital platform

© Published and reproduced with kind permission by Global Legal Group Ltd, London

providers: the state of the existing IT system and its upgradation; training for employees, along with understanding the importance of customer demand from the market; and leadership.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Data Privacy is a main concern in the use of personal data. In September 2013, the MoHFW notified the Electronic Health Record Standards (EHR Standards) for India. They were chosen from the best available, previously used standards applicable to international electronic health records, keeping in view their suitability to and applicability in India. Accordingly, the EHR Standards 2016 document is notified and is placed herewith for adoption in IT systems by healthcare institutions and providers across the country. The MoHFW facilitated its adoption by making available standards such as the Systematised Nomenclature of Medicine Clinical Terminology (SNOMED CT) free-for-use in India, as well as appointing the interim National Release Centre to handle the clinical terminology standard that is gaining widespread acceptance among healthcare IT stakeholder communities worldwide.

In addition, the MoHFW has proposed a new bill, the Digital Information Security in Healthcare Act (DISHA) to govern data security in the healthcare sector. The purpose of this Act will be to provide for electronic health data privacy, confidentiality, security and standardisation. The MoHFW, through the proposed DISHA, plans to set up a statutory body in the form of a national digital health authority for promoting and adopting: e-health standards; enforcing privacy and security measures for electronic health data; and regulating the storage and exchange of electronic health records. In addition, the Personal Data Protection Bill, 2019 was introduced in Lok Sabha, on 11 December 2019 which intends to seek to provide for the protection of the personal data of individuals, and establishes a Data Protection Authority for the same.

4.2 How do such considerations change depending on the nature of the entities involved?

Such considerations are important and usually change with the experience and issues observed during the transition and lag phase between the consumer and service provider.

4.3 Which key regulatory requirements apply?

The MoHFW, through the proposed DISHA, plans to set up a statutory body in the form of a national digital health authority for promoting and adopting: e-health standards; enforcing privacy and security measures for electronic health data; and regulating the storage and exchange of electronic health records. In addition, the National Digital Health Authority (NeHA) under MoHFW is a proposed authority that is intended to be responsible for the development of an integrated health information system in India. It is proposed to be a promotional, regulatory and standard-setting organisation to guide and support India's journey with Digital Health and consequent realisation of benefits of ICT intervention in the health sector. It also spells out the proposed functions and governance mechanism of NeHA. DISHA is the legislation that seeks to formally establish NeHA and facilitate the online exchange of patient information with a view to prevent duplication of work and streamline resources.

4.4 Do the regulations define the scope of data use?

Yes, the regulations define the scope of data use with consent, and also define what is 'sensitive health-related information' and 'sensitive personal information'.

4.5 What are the key contractual considerations?

The primary contractual consideration for data protection would be to enter into non- disclosure and confidentiality agreements with employees which provide remedies in case of disclosure of confidential information.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The key issues in sharing personal data are primarily, but not limited to: the transparency and control of data exchange; security and privacy; and information, trust, responsibility and accountability.

5.2 How do such considerations change depending on the nature of the entities involved?

Such considerations can change during data sharing, particularly data protection and privacy, as this is an important concern.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The MoHFW created the draft for **the Digital Information Security in Healthcare Act** (DISHA) with the aim of securing the healthcare sector data in India, giving people complete ownership of their health data. For example, if you are visiting a doctor for a check-up and the doctor places your results into an electronic health record (EHR) that information is completely protected by DISHA as it is placed within the healthcare system. DISHA proposes three main objectives such as: setting up a digital health authority at national and state levels; enforcing privacy and security measures for electronic health data; and regulating the storage and exchange of electronic health records. Additionally, the draft also provides details on the establishment of **National and State Electronic Health Authorities** (NeHA and SeHA). In effect, it would provide extensive data protection to Indian subjects, as well as govern the data portability.

6 Intellectual Property

6.1 What is the scope of patent protection?

The Patents Act, 1970 provides patent protection in India which is compliant with Trade-Related Aspects of Intellectual Property Rights (TRIPS) and has been adopting and implementing the provisions. To obtain a patent protection in India, apart from the patentability criteria-novelty, inventive step and industrial applicability, the invention must not fall within the ambit of Section 3 and 4 of the Act. As any digital health application works on software and a computer program, Section 3(k) of the Indian Patents Act is relevant which precludes patentability of a computer program *per se*. Recently, the Delhi High Court has

© Published and reproduced with kind permission by Global Legal Group Ltd, London

iterated that all computer programs are not barred under Section 3(k) and when such program demonstrates a 'technical effect' or a 'technical contribution', the invention would be patentable.

Additionally, a patent may not be granted if the program or device is intended to be 'a process for the medicinal, surgical, curative, prophylactic or other treatment of human beings or any process for a similar treatment of animals to render them free of disease or to increase their economic value or that of their products' under Section 3(i) of the Indian Patents Act. However, the device and process of using an *in vitro* mechanism is considered patentable.

6.2 What is the scope of copyright protection?

The Copyright Act, 1957 provides copyright protection in India. A copyright can be applied for original literary, dramatic, musical or artistic work, cinematograph films, and sound recordings. Although the registration of copyright is not essential, it serves as *prima facie* evidence for establishing the right. Digital health application(s) essentially use software and will fall under the definition of 'computer program' and would be protectable under copyright law in India.

6.3 What is the scope of trade secret protection?

There is no exclusive law on dealing with confidential information and trade secrets in India. However, for the developing digital health industry such confidential information is usually protected by signing a mutual agreement such as a non-disclosure and confidentiality agreement.

6.4 What are the typical results on academic technology transfer rules?

Academic technology transfer in digital health and protecting intellectual property is in a nascent stage in India, and now institutions are becoming aware of the importance of protecting and disseminating their knowledge through technology transfer, and the trend seems to be continuing. Typical results on academic technology transfer rules and activities include the following which is not limited to: evaluation/assessment of the invention; protection of intellectual property relating to the technology; and searching and identifying the most suitable partner for licensing and demonstration of the working of the technology.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Section 3(k) of Indian Patents Act precludes patentability of computer program *per se*. Recently, the Delhi High Court has iterated that not all computer programs are included under Section 3(k) when such program demonstrates a 'technical effect' or a 'technical contribution'.

Additionally, a patent may not be granted if the program or device is intended to be 'a process for the medicinal, surgical, curative, prophylactic or other treatment of human beings or any process for a similar treatment of animals to render them free of disease or to increase their economic value or that of their products' under Section 3(i) of the Indian Patents Act. However, the device and process of using an *in vitro* mechanism is considered patentable.

Digital health application(s) essentially use software, thus, they should fall under the definition of 'computer program' and be protected under copyright law in India.

In addition, one of the classes under which a trademark can be registered is class 9, which includes 'computer software and computer programs'.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

For collaborative improvements, various considerations not limited to the following can be practically adopted; such as: primary objectives for such collaboration; details of all eligible members; consideration of management of governance along with dissemination of contract management; confidentiality and evaluation of existing intellectual property and technology transfer; and information regarding the allocation of payments, rights, obligations, liabilities, variations and termination are certain facts for consideration while applying for collaborative improvements.

7.2 What considerations apply in agreements between health care and non-health care companies?

The working concept of healthcare and non-healthcare companies is different in mechanism and approach; however, the prime concern for both sectors is consumer satisfaction. While considering the agreements, the confidentiality protocol for exchange of data and data protection and privacy must also be considered.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning in digital health has the following primary roles:

1. Ease of process to reduce cost, time and efforts.
2. Identifying disease and diagnosis.
3. Drug discovery and manufacturing.
4. To analyse machine learning-based behaviour modifications.
5. To maintain health records.
6. Clinical trial and data collection.
7. Outbreak prediction.

8.2 How is training data licensed?

Currently, India does not have any specific laws for regulation of AI and machine learning and accordingly the activities for these must be in compliance with the existing IT Acts and regulations. In addition, a confidentiality agreement between licensee and licensor can be in place for record.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Currently, this is not applicable in India.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

8.4 What commercial considerations apply to licensing data for use in machine learning?

Authenticity of the licensed data, permission for users, consideration for purpose such as 'know-your customer', restriction on various locations, data privacy and security, quality, rights for using the term and termination are of prime considerations.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

The liabilities that apply to adverse outcome can be civil or criminal in nature and would be different for practitioners running the services and for service providers such as institutes and online suppliers. For civil cases, the remedies are available under the Consumer Protection Act and action as to file a suit before a civil court. In case of negligence by a doctor, a customer can raise a complaint before the ethics committee of the Medical Council of India. Further, criminal liability is dealt with under the provisions of the Indian Penal Code.

9.2 What cross-border considerations are there?

Data localisation is of prime concern.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Primarily the high cost of implementing and maintaining health information technology for digital health is a challenge. Further, security and privacy of data management is another important issue which needs attention.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Besides proper business planning and approach for data privacy and security, non-healthcare companies must understand that the health sector follows highly regulated standards for manufacturing and marketing. Additionally, for the healthcare market consumer laws are also applicable.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

Some of the key issues that venture capital and private equity firms should consider before investing in digital health care ventures are: proper business plan; market opportunity; strategic partnership; understanding of financial and key matrices for business; potential risk for business; expected valuation; and IP protection.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Rajeev Kumar, Partner, is a registered Indian patent attorney and holds a Master's degree in Pharmaceutical Sciences. He leads the Patent Filing and Prosecution Group at LexOrbis and has more than 15 years of experience. He assists clients in mining and securing patent protection in India, Europe, USA, internationally and assists other countries in drafting and prosecuting patents in relation to pharmaceuticals, neutraceuticals, chemical, biochemical, organic chemistry, peptide chemistry, medicinal products, medical devices, oil and gas, and nanotechnology. He is also engaged in providing product or process clearance opinions to clients in India and providing guidance in conducting freedom to operate searches in other jurisdictions. He also provides assistance to the legal team in various contentious matters, including pre-grant and post-grant oppositions, revocations and appeals before IPAB and in litigation cases before the courts. He is a regular speaker in various seminars/conferences and has published a number of articles on various patent-related subjects.

LexOrbis
709–710 Tolstoy House
15–17 Tolstoy Marg
New Delhi –110001
India

Tel: +91 11 2371 6565
Email: rajeev@lexorbis.com
URL: www.lexorbis.com

Pankaj Musyuni is a Managing Associate at LexOrbis. He is an advocate registered with the Bar Council of India, and a patent agent. He holds a Master's degree in pharmaceutical science and management. He regularly advises clients on IP strategy and portfolio management. He has in-depth knowledge of patent law and regulatory framework and extensive experience in patent filing, drafting, prosecution and advisory matters – especially pertaining to the field of chemical, pharmaceutical and start-ups. He has authored several articles and delivered talks at various forums on patent law practice, regulatory landscape and clinical research.

LexOrbis
709–710 Tolstoy House
15–17 Tolstoy Marg
New Delhi –110001
India

Tel: +91 11 2371 6565
Email: pankaj@lexorbis.com
URL: www.lexorbis.com

LexOrbis is a premier law firm, and one of the fastest growing IP firms in India, with offices in three strategic locations: Delhi; Mumbai; and Bengaluru. With a team of over 85 highly reputed lawyers, engineers and scientists, we act as a one-stop shop and provide practical solutions and services on all Intellectual Property and legal issues faced by technology companies, research institutions, universities, broadcasters, content developers and brand owners. Our services include Indian and global IP (patents/designs/trademark/copyright/GI/plant varieties) portfolio development and management, advisory and documentation services on IP transactions/technology-content transfers and IP enforcement and dispute resolutions at all forums across India. We have a global reach with trusted partners and associate firms.

www.lexorbis.com

LexOrbis INTELLECTUAL PROPERTY ATTORNEYS

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Ireland


Michaela Herron


Brian McElligott


Brian Johnston


John Farrell

Mason Hayes & Curran

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no standardised definition of "digital health" in Ireland. Digital health is generally considered to consist of electronic information, interactions and products that connect people and communities to health services. Generally, the tools and services use information and communication technologies ("ICTs") to improve prevention, diagnosis, treatment, monitoring and management of health and lifestyle.

1.2 What are the key emerging technologies in this area?

- AI: The use of AI, machine learning and predictive analysis in the healthcare and life sciences industry is becoming increasingly common (e.g. software systems which can analyse large volumes of data and provide disease predictions or risk profiles from that data).
- Wearables: These are mobile devices that are worn directly on the body which collect physiological data and conduct an analysis on that data – sometimes with or without an associated app.
- Telemedicine: This relates to the delivery of healthcare services over digital platforms or apps (for example, online doctor's consultations, counselling services conducted through a communication app, etc.).
- Health Apps: There are a significant volume of apps on the market which provide health information or services (examples include prescribing assistance apps, early detection apps and dermatology review apps).

1.3 What are the core legal issues in health care IT?

Given the protection of health data as a special category of data under the GDPR, data protection and cybersecurity are a key legal issue in healthcare IT. In addition, patient safety is paramount, and any systems, products and software used, must ensure that patient safety is appropriately maintained. Product classification and determining whether a digital health product or device is a medical device or not is also a key legal issue.

2 Regulatory

2.1 What are the core health care regulatory schemes?

Healthcare Framework

- The Health Act 2004.
- The Health Act 2007.

Regulation of Healthcare Practitioners

- The Medical Practitioners Act 2007 regulates the medical profession in Ireland.
- The Nurses and Midwives Act 2011 regulates nurses and midwives in Ireland.
- The Pharmacy Act 2007 regulates pharmacists and pharmaceutical assistants.
- The Health and Social Care Professionals Act 2005 (currently regulates dietitians, dispensing opticians, medical scientists, occupational therapists, optometrists, physical therapists, physiotherapists, radiographers, radiation therapists, social workers, and speech and language therapists). In time, the Health and Social Care Professionals Act 2005 will also regulate clinical biochemists, counsellors, orthoptists, podiatrists, psychologists, psychotherapists and social care workers.

Medical Devices

The regulatory regime for medical devices is of significance to a high volume of digital health products. The Medical Devices Directive (Directive 93/42/EEC) (the "MDD") is implemented in Ireland by the European Communities (Medical Devices) Regulations 1994 and will be replaced from 26 May 2020 by the EU Medical Devices Regulation (Regulation 2017/745) (the "MDR"). In addition, the *In Vitro* Diagnostic Medical Devices Directive (Directive 98/79/EC) is implemented in Ireland by the European Communities (*In Vitro* Diagnostic Medical Devices) Regulations 2001 and will soon be replaced by the In Vitro Diagnostic Regulation 2017/746 (the "IVDR").

2.2 What other regulatory schemes apply to digital health and health care IT?

There is a lack of legislation and regulatory schemes specific to digital health IT and eHealthcare in Ireland. However, a number of different regimes may be applicable depending on the type of digital health product involved.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

There is an independent body known as **eHealth Ireland** that was set up in 2013, initially as part of the Health Service Executive. eHealth Ireland has developed a strategy demonstrating how citizens, the Irish healthcare delivery systems – both public and private – and the economy as a whole will benefit from eHealth. eHealth Ireland works closely with all of the key business organisations within the health service, in order to drive forward the eHealth strategy and ensure that key IT systems are implemented on time and to budget.

The **General Product Safety Directive** 2001/95/EC (implemented in Ireland by the General Product Safety Regulation 2004) may apply to digital health products which are not classified as medical devices under the MDD or MDR.

The **General Data Protection Regulation** ("GDPR") has general application to the processing of personal data in the European Union, setting out more extensive obligations on data controllers and processors, and providing strengthened protections for data subjects. Although the GDPR is directly applicable as a law in all Member States, it allows for certain issues to be given further effect in national law. In Ireland, the national law, which, amongst other things, gives further effect to the GDPR, is the **Data Protection Act 2018**.

The **Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018** outline the mandatory additional measures that must be implemented and taken by those using personal data for the purposes of "health research". The measures include obtaining explicit consent from the individual involved in the research, or obtaining approval from a research ethics committee where consent cannot be obtained and there is a public interest in conducting the research even absent explicit consent.

The Directive on security of network and information systems (the "**NIS directive**") (Directive 2016/1148), adopted in July 2016, is the first piece of EU-wide legislation on cybersecurity and entered into force in August 2016. It provides legal measures to boost the overall level of cybersecurity in the EU. It represents a significant change in how countries in the EU approach cybersecurity and involves a shift in approach towards a more formal type of regulatory relationship in certain key industries.

In Ireland, the NIS directive was signed into Irish law on the 18 September 2018 by way of Statutory Instrument No. 360 of 2018.

The **Consumer Protection Act 2007**, which implements EU Directive on Unfair Commercial Practices (Directive 2005/29/EC), may also be applicable to digital health products that are intended for consumer's use.

Finally, the regulatory regime for medicines may also be applicable if the digital health product is involved with medicine or medicine delivery. The regulatory regime in relation to medicines is primarily governed by **Directive 2001/83EC** on the Community code relating to medicinal products for human use and implemented through various national regulations.

2.3 What regulatory schemes apply to consumer devices in particular?

For consumer devices that are not considered medical devices and are therefore subject to the medical devices regulatory framework, the most relevant regulatory schemes are likely to be:

- General Product Safety.
- Data Protection.
- Consumer Protection.
- Product Liability.
- Intellectual Property.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The **Health Products Regulatory Authority** (the "HPRA") derives its regulatory authority from the Irish Medicines Board Act 1995 and the Irish Medicines Board (Miscellaneous Provisions) Act 2006. The HPRA has the authority to regulate health products in Ireland. This role includes regulation of human and veterinary medicines, human blood, tissues and cells, cosmetic products, medical devices, active pharmaceutical ingredients, and controlled drugs and substances. The HPRA have broad powers including the right to investigate, inspect, compel information and prosecute as well as refuse and revoke licences.

The **Competition and Consumer Protection Commission** (the "CCPC") is an Irish State Agency set up in October 2014. It combines the previous functions of the Competition Authority and the National Consumer Agency (the "NCA") namely enforcing competition and consumer protection law in Ireland. This includes enforcement of product safety regulations and assessment of mergers. The NCA derived their authority from the European Communities (General Product Safety) Regulations and the Consumer Protection Act 2007.

The **Health and Information Quality Authority** ("HIQA") was established under the **Health Act 2007** and is an independent authority that exists to improve health and social care services for the people of Ireland. In October 2019, HIQA published a Guide to a review programme of eHealth services in Ireland. HIQA have established a new review programme to monitor compliance with National Standards for Safer Better Healthcare for eHealth services within the HSE in Ireland, specifically in respect of patient safety and data quality.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

Registered healthcare practitioners are the subject of professional regulation and must ensure that their practice is in compliance with their governing legislation and, where applicable, codes of conduct and ethical guides.

In relation to digital health products, a key concern for regulatory authorities is patient safety. The safety expected from digital health products will depend on the product and what regulatory regime it sits under. As a general rule, regulatory authorities (either the CCPC or HPRA), will investigate breaches of product safety – whether it arises under the Medical Devices framework or the general product framework.

In addition, given that a large volume of digital health products contain, store, process or use health data, the Data Protection Commissioner will generally investigate any data breaches and may take appropriate enforcement action.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

The MDD, IVDD, MDR and IVDR regulate software as a Medical Device.

Under the MDR, the definition of a medical device includes software which is designed for the purposes of prediction and prognosis.

Rule 11 of the MDR specifically addresses software and provides a classification system for determining the status of software. The classifications under the MDR are:

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Class IIa – Software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes except if such decisions have an impact that may cause:

- death or an irreversible deterioration of a person's state of health, in which case it is classified as **Class III**; or
- a serious deterioration of a person's state of health or a surgical intervention, in which case it is classified as **Class IIb**.

Software intended to monitor physiological processes is classified as **Class IIa**, except if it is intended for monitoring of vital physiological parameters where the nature of variations of those parameters is such that it could result in immediate danger to the patient in which case it is classified as **Class IIb**.

All other software is classified as **Class I.**

Approval for clinical use is assessed by either the manufacturer (if the class of device is subject to a self-certification conformity procedure) or a Notified Body.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Regulation of both medical practitioners involved in Telehealth services and whether the medical mevices framework is applicable are both core issues. In addition, issues around cybersecurity, data protection and liability are also relevant.
- **Robotics**
  Liability and the scope of contractual related issues such as service standard, availability and maintenance remain key issues in robotics. Intellectual property issues can also arise.
- **Wearables**
  The medical devices framework is a core issue for wearables, along with general data protection, cybersecurity and consumer protection laws. Product safety and liability issues can also arise.
- **Virtual Assistants (e.g. Alexa)**
  Data protection and cybersecurity concerns are one of the main issues affecting the use of virtual assistants, particularly given the "always on" nature of the product. Liability and product safety issues can also arise relating to the use of these products and how they interact with other smart devices.
- **Mobile Apps**
  See Telehealth and Wearables.
- **Software as a Medical Device**
  The medical devices framework will apply to software that is classified as a medical device. Issues relating to data protection, cybersecurity and consumer protection are also relevant.
- **AI-as-a-Service**
  Data protection and cybersecurity are key issues, particularly related to any international transfers of data. Consumer protection, liability and general contractual matters will also be important.
- **IoT and Connected Devices**
  Cybersecurity and data protection, particularly related to the "always on" nature of these devices as well as the integrity of the device security from unauthorised access attempts, are core issues. Liability and consumer protection principles are also important.
- **Natural Language Processing**
  Natural language processing typically gives rise to data protection concerns if the data is not sufficiently anonymised. Additionally, intellectual property and the ownership of inputs and outputs of the system are important. Contractual issues such as service availability and liability issues can also arise.

3.2 What are the key issues for digital platform providers?

The future regulation of digital platforms remains one of the key objectives of the recently appointed European Commission. In particular, it is expected that there will be a focus by EU lawmakers on issues such as the regulation of online harm and also a recasting of the long-standing liability rules which currently provide for broad liability safe harbours for digital platforms.

In addition to the types of legal issues faced by other digital service providers such as data protection, consumer protection and contractual related issues, there have also been recent changes relating to fairness and transparency which will take effect on 12 July 2020. The EU Regulation on providing fairness and transparency for business users of online intermediation services (EU 2019/1150) creates a framework for minimum transparency and redress rights. The transparency provisions will require digital platform providers to:

- set out in their terms and conditions the main parameters determining ranking;
- the reasons for the relative importance of those main parameters as opposed to other parameters; and
- the extent the ranking is influenced by payments, direct or indirect.

The digital platform must set out an easily and publicly available description of the parameters, drafted in plain and intelligible language, and kept up to date on the platform website. Where the digital platform alters the ranking order in a specific case or delists a particular website following a complaint or notification from third party notification, the platform provider must allow the business user/corporate website user to inspect the complaint or notification.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The use of personal data is subject to the GDPR. The key issues to consider before using personal data are set out:

- **Transparency:** Personal data must be processed fairly and transparently. Data controllers must provide certain minimum information to data subjects regarding the processing of their personal data. This information must be communicated to the data subjects in a concise, transparent, intelligible and easily accessible manner, using clear and plain language.
- **Lawful basis for processing:** There must be a lawful basis for processing – at least one of the following must apply whenever personal data is processed: data subject consent; contractual necessity; legal obligation; vital interests of the data subject; necessary for the purposes of a task carried out in the public interest; or necessary for the

© Published and reproduced with kind permission by Global Legal Group Ltd, London

purposes of legitimate interests of the data controller or third parties.

- **Purpose limitation:** Personal data must be collected for specified explicit and legitimate purposes. It cannot be further processed in a manner incompatible with those purposes.
- **Data minimisation:** Personal data must be adequate and relevant under the GDPR. The GDPR also requires that personal data is limited to what is necessary in relation to the purposes for which the data is processed. An organisation may have to review its data processing operations in order to ascertain whether it processes any personal data which is unnecessary in respect of the relevant purpose for which processing is carried out.
- **Accuracy:** Personal data must be accurate, and where necessary, kept up to date. Reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay.
- **Storage limitation:** Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary.
- **Integrity and confidentiality:** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability:** Accountability is a new concept introduced by the GDPR: it requires controllers to be able to demonstrate how they comply with the data protection principles listed, including by implementing policies. This is significant as it shifts the burden of proof to the data controller in the event of a compliance investigation by a data protection authority.

Additional considerations apply where there is processing of a special category of data, such as health data, biometric data (where it is used to uniquely identify an individual) and genetic data. A data controller can only process a special category of data lawfully under the GDPR if:

i. there is a lawful basis for processing; and
ii. one of the exceptions under Article 9(2) GDPR applies. An example of a valid exception is where the data subject has explicitly consented to the processing of their special category data.

4.2 How do such considerations change depending on the nature of the entities involved?

If more than one entity is involved in using data, this can give rise to contractual considerations, as explained in questions 4.5 and 5.1.

Public bodies are subject to additional statutory obligations in relation to sharing of data, as explained in questions 5.2 and 5.3.

4.3 Which key regulatory requirements apply?

The key data protection legislation in Ireland is GDPR, as implemented and supplemented by the Data Protection Acts 1988 to 2018 (collectively the "DPA").

Other health sector-specific regulatory requirements are found in:

- S.I. No. 188/2019 – Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2019;
- S.I. No. 314/2018 – Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018; and
- S.I. No. 82/1989 – Data Protection (Access Modification) (Health) Regulations 1989. This legislation sets out certain restrictions in relation to the right of access to health data.

4.4 Do the regulations define the scope of data use?

The regulations outlined above set the legal boundaries for lawful data use by a person established in Ireland regardless of whether that use of data occurs in Ireland or beyond.

The regulations also create additional rules regarding the transfer by a person established in Ireland outside the European Economic Area (or other territories deemed to ensure an adequate level of protection) (a "Transfer"). A person needing to conduct a Transfer needs to ensure compliance with these additional rules, including, for example, by ensuring the Transfer is carried out pursuant to the EU Commission's Standard Contractual Clauses ("SCCs") Commission, Binding Corporate Rules ("BCRs") or one of the derogations provided for by the regulations, such as data subject consent or contractual necessity.

4.5 What are the key contractual considerations?

Key contractual considerations come into play when a data controller appoints a data processor to process personal data on its behalf. The data controller and data processor must enter into a written agreement (a Data Processing Agreement, or "DPA") which sets out the subject matter and the duration of the processing, the nature and purpose of the processing, the type of personal data being processed, the categories of data subjects and the obligations and rights of the controller.

The contractual terms must stipulate that the processor:

i. only acts on the documented instructions of the controller;
ii. imposes confidentiality obligations on all employees;
iii. ensures the security of personal data that it processes;
iv. abides by the rules regarding the appointment of sub-processors;
v. implements measures to assist the controller with guaranteeing the rights of data subjects;
vi. assists the controller in complying with its obligations regarding security, including notifying the data controller of any personal data breaches and providing assistance, and conducting data protection impact assessments and any prior consultation required with the regulator;
vii. either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and
viii. provides the controller with all information necessary to demonstrate compliance with its obligations under the agreement.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

There are no additional statutory requirements to consider when sharing personal data (save in the respect of public bodies, as below). However, in the event two parties are sharing personal data and, in addition, jointly determining the purposes and means for which that shared data will be processed, there will be a requirement to enter into a joint controller agreement. This agreement must determine the respective responsibilities for

© Published and reproduced with kind permission by Global Legal Group Ltd, London

compliance with the obligations under this Regulation for each controller, including the role of each controller with respect to the relevant data subjects. The essence of the agreement must be made available to the data subjects.

For public bodies, in addition to those set out above, the Data Sharing and Governance Act 2019 was passed into law in March 2019 but has yet to come into force in its entirety. Once in force, it will impose additional obligations on public bodies before sharing data. The Data Protection Commission has also issued guidance for public bodies on steps to take prior to sharing data.

5.2 How do such considerations change depending on the nature of the entities involved?

Additional considerations apply to public sector bodies, as explained above.

5.3 Which key regulatory requirements apply when it comes to sharing data?

There are no additional regulatory requirements other than those set out above for private sector entities (including as set out in question 4.3).

As explained above, for public sector entities, in addition to those set out above, the Data Sharing and Governance Act 2019 was passed into law in March 2019 but has yet to come into force in its entirety.

6 Intellectual Property

6.1 What is the scope of patent protection?

Under Section 9(1) of the Patents Act 1992, an invention is patentable if it is susceptible of industrial application, is new and involves an inventive step.

The 1992 Act explicitly states that the following are not patentable:

a) a discovery, scientific theory or a mathematical method;
b) an aesthetic creation;
c) a scheme, rule or method of performing a mental act, playing a game or doing business, or a program for a computer;
d) the presentation of information;
e) a method for treatment of the human or animal body by surgery or therapy and a diagnostic method practised on the human or animal body;
f) a plant or animal variety or an essentially biological process for the production of plants or animals other than a micro-biological process for the products thereof; and
g) an invention whose commercial exploitation would be contrary to public order or morality.

6.2 What is the scope of copyright protection?

To obtain protection, the work must be original in accordance with the Copyright and Related Rights Act 2000 ("CRRA"). The protection only applies to works, and not ideas. It subsists automatically on creation, as soon as the idea is fixated, for example, on paper, film or other mixed mediums such as CD-ROM, DVD, or on the Internet. Registration is not required. The copyright owner is granted the following:

- reproduction rights;
- making available rights;
- distribution rights;
- rental and lending rights; and
- adaptation rights.

6.3 What is the scope of trade secret protection?

The European Union (Protection of Trade Secrets) Regulations 2018 defines the scope of protection of trade secrets by reference to three essential ingredients:

- the information must be secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, be generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- the information must have commercial value because it is secret; and
- the information must have been subject to reasonable steps under the circumstances, by the trade secret owner, to keep it secret.

This excludes trivial information and the normal experience and skills gained by employees.

6.4 What are the typical results on academic technology transfer rules?

Typically, results and intellectual property produced in Irish universities are licensed to spin out university companies or industry partners on an exclusive basis in return for annual royalties and on the basis of model agreements produced and managed by Knowledge Transfer Ireland (https://www.knowledgetransferireland.com). Assignments of such results and intellectual property may also be procured so long as the transfer is in accordance with State Aid rules.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Apart from any granted patent and/or trade secrets falling within the scope of the response to question 6.4 above, it is most likely the scope of copyright in the software/computer program. This extends only to the form of expression of the software/computer program itself. The copyright does not extend to the ideas and principles underlying the computer program (section 17(3), CRRA). In practice, this means that the functionality of the particular piece of software in the medical device is not protected by copyright in a computer program, absent literal copying of the source code.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

7.1.1 Intellectual Property

Parties working jointly on projects which may lead to the creation of new, or modified intellectual property (IP), should enter into a written contractual arrangement which clearly sets out each party's respective ownership of any existing IP (or background IP) and any created or modified intellectual property (newly developed IP). Additionally, the parties should also determine each party's right to use the other party's background

© Published and reproduced with kind permission by Global Legal Group Ltd, London

IP, as well as any newly developed IP. This is particularly the case in relation to regulating any potential future commercial exploitation.

On a practical note, it may be difficult for parties to manage jointly owned IP, and consideration should be given to how decision making in respect of any jointly owned IP might work, before opting for this in a contract.

If any assignment of IP is required as part of a project, Irish law requires that any such assignment be in writing and as such an oral arrangement would likely be ineffective.

7.1.2 Liability

The parties should also determine (preferably by way of written agreement) the liability of each party for any damage caused by "collaborative improvements" or created/modified IP. We would typically expect that liability attaches to the party who owns and/or licenses the IP; however, this should be carved out appropriately, taking into consideration the relevant circumstances. For example, liability for non-licensed use of a digital health product may be excluded.

7.2 What considerations apply in agreements between health care and non-health care companies?

Parties will need to give particular consideration to the warranties, liability, indemnity and limitation clauses in a contract (or their absence if that is the case). Suppliers of digital health services may seek to provide limited guarantees in respect of the standard or availability of the service, and care should be taken to ensure that any such limitation is not overly broad, and that the supplier has not included an unreasonably low cap on liability in respect of unavailability of the service.

In respect of liability, parties should also be aware that if they are contracting in respect of a "product" within the definition of the Product Liability Directive, then a strict liability regime will apply, where the necessary proofs have been established, to the developers or manufacturers (and potentially the suppliers or distributors).

Consumer law also restricts the extent to which liability towards consumers can be limited and parties should bear this in mind as part of the negation of upstream. If the product incorporates artificial intelligence (AI) technology, the legal landscape in respect of liability is currently unclear. We expect to see a new approach to liability clauses in the near future as this area of law develops.

Parties should also give careful consideration to their confidentiality and audit rights under a contract. If the relevant product or service incorporates AI, the supplier may be reluctant to grant audit rights which provides access to information which it deems to be confidential or proprietary in nature (for example, how its AI system operates). Contrastingly, the customer (which may be a healthcare body) may require robust audit rights, particularly if sensitive health data is being processed using the supplier's product or service. In respect of confidentiality, a customer may require clear assurances that confidential information (for example, personal data) is removed from the supplier's AI system on a regular basis or at the end of the relationship. A supplier may be reluctant to agree to this as (a) it may be practically difficult to do and (b) it may negatively affect its AI system, which may have been designed to learn from the information that it is processing.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning currently plays an important role in digital health in the area of medical diagnostics, clinical trials and surgery.

An example of a recent development in Ireland can be found in University College Cork, where machine learning techniques are being developed by researchers that will analyse neonatal electrical brain patterns and combine this data with other vital sign information to provide an overall brain health index for new-born babies.

This expanding scope of application of machine learning is and will continue to challenge regulators and manufacturers alike, especially with regard to compliance under the MDD and MDR.

8.2 How is training data licensed?

Depending on the nature of the dataset, it may qualify as a trade secret/know-how or for some form of copyright protection, i.e. an original database work or *sui generis* database right under the Copyright and Related Rights Act 2000 ("2000 Act"). In most cases of bulk raw data, the dataset will not be covered by copyright. In any event, the data is likely to be licensed by the data owner under standard written terms taking into account scope, field of use, sublicensing, warranties and obligations on expiry. Under the 2000 Act, an "*Original Database*" is defined as a "*database in any form which by reason of the selection or arrangement of its contents constitutes the original intellectual creation of the author*".

The Irish Government provides open and training (non-personal) data, sourced from the activities of public bodies under their *Open Data Strategy 2017-2022*. Data and metadata provided under the strategy are licensed using the Creative Commons (CC-BY) Licence. Data and content licensed under the Creative Commons (CC-BY) Licence can be mined for commercial and non-commercial research purposes.

The EU recently adopted the third version of the Directive on Public Sector Information (Directive (EU) 2019/1024) which aims to promote the use of "open data" sets for both commercial and non-commercial exploitation. Ireland has until 16 July 2021 to implement the Directive.

The EU also recently enacted the Copyright Directive (Directive EU 2019/790) which introduces a copyright exception for text and data mining for non-commercial scientific research in certain circumstances. Ireland has until mid-2021 to enact this directive into national law.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

The key IP rights that will arise in these circumstances will be the copyright in the developed software. Under Section 2 of the 2000 Act, a "computer-generated" work is one that is generated by a computer in circumstances where the author of the work is not an individual. The author of this type of work according to Section 21(f) of the 2000 Act is the person by whom the

© Published and reproduced with kind permission by Global Legal Group Ltd, London

arrangements necessary for the creation of the work are undertaken. There is no case law on this point in Ireland as yet.

At present, under Irish law it is likely that the data scientists and software engineers putting together the models and software which improve the algorithms would be individually and collectively considered the "authors" and first owners of the IP rights to these improved algorithms.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Parties to a licence concerning a training data set for use in machine learning may wish to consider the following:

- Whether they wish for the data set to be licensed for a particular purpose or purposes only. How the parties will treat any improvements to the algorithm/software on foot of use of the training data.
- What steps the licensee is obligated to take to protect the data and the licensor's and licensee's potential liability if a data breach occurs.
- Licensors will often seek to disclaim any representation or warranty with respect to the completeness, accuracy, timeliness or utility of the licensed data.
- Whether the licensee will require use of the data set for a limited time or whether the perpetual licence for the data set will be required.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Product Liability under Statute

The principal piece of legislation is the Liability for Defective Products Act 1991 (1991 Act). This implements Directive 85/374/EEC on liability for defective products. The 1991 Act holds a producer strictly liable in damages in tort for "damage caused wholly or partly by a defect in his product". Section 5 of the 1991 Act provides that a product is considered "defective" if it does not provide the safety that a person is entitled to expect.

Product Liability under Tort

A party may also be found liable under the tort of negligence for a defective product where a duty of care was owed by that party (such as the manufacturer or seller) and there was a breach of that duty of care and this breach caused damage.

Contract

There are also contractual obligations which must be considered. The sale of goods is governed by the Sale of Goods Act 1893 and the Sale of Goods and Supply of Services Act 1980 (the "Acts"). The Acts imply a condition into a contract for the sale of goods that the goods supplied under the contract must be of "merchantable quality" (that is, that they are as fit for the purpose or purposes for which goods of that kind are commonly bought and as durable as it is reasonable to expect having regard to any description applied to them, the price (if relevant) and all the other relevant circumstances). Clearly, if the product sold is subsequently not of merchantable quality, the seller will be in breach of this implied term in the contract.

The European Communities (Certain Aspects of the Sale of Consumer Goods and Associated Guarantees) Regulations 2003 (2003 Regulations) apply to contracts for the sale of goods to consumers. This is in addition to the Acts discussed above. The 2003 Regulations require that goods delivered under a contract of sale to the consumer must be in conformity with that contract.

Liability may also arise through contractual relations entered into between various parties using or supplying a digital health product – e.g. hospital, clinician, hardware manufacturer, software manufacturer, etc. Parties entering into a contract should be highly conscious of their respective liability positions.

Criminal

The European Communities (General Product Safety) Regulations 2004 (2004 Regulations) implement the EU General Product Safety Directive. These Regulations make it an offence to place a product on the market unless it is a safe product. A safe product is "any product which under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons".

The 2004 Regulations provide that a failure of producers or distributors to inform the national consumer authority, the Competition and Consumer Protection Agency, where they know, or ought to know, that a product which has been placed on the market by them is incompatible with safety requirements, is a criminal offence.

Medical Devices

A number of digital health products will be medical devices and subject to liability and offences arising under the MDD and MDR. For example, it is an offence to place a non-CE marked medical device on the market.

Clinical Negligence

Given the nature of digital health products, it is important to remember that medical practitioners will frequently be involved in using these products or delivering healthcare services which are dependent on these products. Therefore, the issue of clinical negligence must be considered. In Ireland, clinical negligence will be established where:

- a medical practitioner owed a patient a duty of care;
- that duty of care was breached (as the standard of care delivered fell short of that expected); and
- damage or injury was suffered as a result.

9.2 What cross-border considerations are there?

Forum shopping may occur in litigation involving digital health products or services. Claimants can seek to use any differences between the laws and/or procedures of member states to their advantage. However, they may find that the choice-of-law rules of the chosen forum require the laws of a different member state to be applied. Even if similar actions are initiated in different member states against the same defendant(s), there is no procedure to consolidate those actions.

Forum shopping can occur under the Recast Brussels Regulation (Regulation EU 1215/2012). For example:

- Consumers can choose to bring claims in the defendant's member state or the member state in which they are domiciled.
- For contractual claims, the claim may be brought in the courts for the place of performance of the obligation in question. In relation to contracts for the sale of goods, unless otherwise agreed, the place of performance is a member state where the goods are delivered.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- For claims relating to negligence or other torts, the claim may be brought in the courts for the place where the harmful event occurred.
- The Hague Convention on Choice of Court Agreements (Hague Convention) entered into force in all EU member states on 1 October 2015 (except Denmark where it was entered into force on 1 September 2018). However, the Hague Convention will have limited effect in many liability claims relating to digital health products as it does not apply to choice of court agreements involving consumer contracts (whether concerning consumer to consumer or business to consumer transactions), personal injury claims or tort claims relating to tangible property.

Finally, in 2017 the EU introduced the New Deal for Consumers, with the aim of strengthening consumer rights and to remove obstacles to consumer redress across the EU. This was a significant step forward in modernising and harmonising EU consumer law, by empowering qualified bodies to take representative action on behalf of consumers, as well as giving stronger sanctioning powers to consumer authorities in all member states.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Regulatory compliance and reliability remain two of the biggest issues for cloud-based digital health services. The GDPR creates a strong regulatory regime in respect of health data as outlined in further detail in the response to question 4.1. In particular, restrictions on the transferring of health data outside the European Economic Area create a conflict with the traditional cloud-based service model. As a result, customised solutions are often required which can add an additional layer of complexity and expense.

Reliability also remains a key issue for cloud services, particularly the ability for the customer to implement its own business continuity, disaster recovery and service availability standards on to suppliers of standardised cloud services.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Non-healthcare companies need to be aware of the regulatory regimes applicable to the digital health product or service they are providing. Awareness of their regulatory regimes and identifying their relevant obligations should be done at an early stage and be considered throughout all stages of product development.

If the digital health product uses personal data or indeed health data, companies must ensure compliance with the GDPR to ensure that all data is being handled in accordance with GDPR requirements.

Finally, patient safety must remain at the forefront of companies' minds as this is an issue that regulators will carefully scrutinise.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

Clearly investors should be highly cognisant of the company's financial performance, sustainability and scalability of the product(s) and indeed organisation. However, investors should also be particularly aware that digital healthcare is governed by a complex legal and regulatory environment which includes obligations in relation to data, cybersecurity, consumer protection, product regulation, product safety, intellectual property and healthcare practitioners.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Michaela Herron is a Regulatory Partner who advises clients in the pharmaceutical, medical device (including software medical device), healthcare, digital health, cosmetic and general consumer produce sectors on various regulatory compliance matters, including regulatory approval, labelling, traceability, safety and liability issues. She has advised clients on enforcement action, including the defence of criminal prosecutions, the implementation and coordination of produce withdrawals and product recalls and rectification strategies in multiple jurisdictions. She has also acted on behalf of clients in significant commercial disputes, group product liability litigation, inquests, injunctive relief and judicial review proceedings.

Mason Hayes & Curran
South Bank House
Barrow Street, Dublin 2
Ireland

Tel: +353 1 614 2199
Email: mherron@mhc.ie
URL: www.mhc.ie

Brian McElligott advises on complex IP and technology issues for clients from a range of sectors including digital health, pharma, food, beverage, energy and agriculture. He also advises on artificial intelligence (AI) across those sectors and plays an active role in the National Strategy on AI for Ireland and with the AI Alliance at EU level. He works closely with clients on the formulation and implementation of effective IP development and protection strategies. This includes guiding international brand owners through complex IP protection and commercialisation issues and advising major technology companies on IP licensing and due diligence surrounding mergers, acquisitions, IPOs and foreign direct investment. Brian is a registered Irish and European Union trade mark and design agent and has a wealth of experience of managing significant trade mark portfolios of major international clients. He is a former Chair of the Licensing Executives Society of Ireland and the Irish branch of the Anti-Counterfeiting Group.

Mason Hayes & Curran
South Bank House
Barrow Street, Dublin 2
Ireland

Tel: +353 1 614 2199
Email: bmcelligott@mhc.ie
URL: www.mhc.ie

Brian Johnston is a Partner on the firm's Privacy and Data Security team. Brian provides companies with solutions to their privacy and data protection problems. His focus is on helping some of the world's leading technology companies to launch new and innovative technologies in Europe, including in the digital health sector. This includes helping companies to navigate the risks associated with the collection and use of health data, conducting health research and the anonymisation and commercialisation of data. Brian also has particular expertise advising companies throughout their engagement with regulators and law enforcement agencies, including helping them to resolve complex investigations and enforcement action. Prior to joining the firm, Brian gained much of his experience with a leading technology firm in London and in-house at Samsung as its European Data Protection Officer. He also gained valuable experience working in the Irish Data Protection Commission a number of years ago.

Mason Hayes & Curran
South Bank House
Barrow Street, Dublin 2
Ireland

Tel: +353 1 614 2323
Email: bjohnston@mhc.ie
URL: www.mhc.ie

John Farrell is a Partner on our Commercial team and practises as part of the Technology, Consumer Law, Media & Telecoms and Privacy & Data Security teams. John works closely with some of the world's largest companies solving complex technology law issues and providing commercially focused solutions. He specialises in advising on large-scale commercial arrangements, including multi-party structures involving various contractual agreements. John also provides strategic and contractual guidance on privacy issues, including international data flows, vendor management and internal compliance programmes, as well on consumer law issues, including helping companies launch innovative products within the complex and highly regulated consumer law realm.

Mason Hayes & Curran
South Bank House
Barrow Street, Dublin 2
Ireland

Tel: +353 1 614 2323
Email: jfarrell@mhc.ie
URL: www.mhc.ie

Mason Hayes & Curran is a business law firm with 90 partners and over 500 staff. We understand the challenges international organisations face when investing or locating in a foreign country. We assist them during initial establishment and in meeting their ongoing legal and commercial imperatives. We have offices in London, New York and San Francisco, three of Ireland's most important conduits for inward investment to Ireland. Corporate social responsibility is a natural fit with the way we do business. We invest in our society and communities through a range of focused programmes.

www.mhc.ie

MASON HAYES & CURRAN

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Israel


Eran Bareket


Alexandra Cohen

Gilat, Bareket & Co., Reinhold Cohn Group

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no general definition of "digital health" in Israel. However, the definition can be derived from the government's "National Digital Health Plan as a Growth Engine" approved on 25 March 2018, which defines digital health as follows: "*The vision of the digital health strategy as published by the Ministry of Health is to enable a leap in the healthcare system so that it will be a sustainable, advanced, innovative, renewable and constantly improving health system, by leveraging the best available information and communication technologies.*"

Although there is no legal definition, the digital health sector is very developed in Israel and there are hundreds of innovative companies – including start-ups – dealing with digital health and developing technologies in different digital health sectors.

1.2 What are the key emerging technologies in this area?

The key emerging technologies in digital health in Israel include digital tools and platforms that enable consumers to proactively track, manage and treat their own medical conditions, as well as digital tools of remote monitoring, decision support, clinical workflow, diagnostics, patent engagement and assistive devices.

For example, ContinUse Biometric Ltd. is an Israeli company that developed methods using AI techniques for nano-level detection and analysis of vibrations associated with the movement of internal organs and molecules. This technology enables the continuous measurement of vital signs and other bio-parameters (such as heart and respiration rates and blood pressure) from a distance and with high accuracy.

1.3 What are the core legal issues in health care IT?

The core legal issues in health are:

- How conventional healthcare regulation is to be applied to digital health services.
- Secondary use of health data and how it is de-identified (determining standards of de-identification/hiding identity) – currently regulated in part by the Director-General circular on secondary uses of health data.
- Ownership of health data and rights of use.
- Ownership of products developed based on health data.
- Rights of state hospitals and healthcare organisations to hold equity in startups.
- Privacy protection of holders of health data – regulated by the Protection of Privacy Law, 5741-1981 and the Protection of Privacy Regulations (Data Security) 5777-2017.
- Creating a uniform platform for collaborations based on databases of different entities (competition law, standardisation of information, etc.).

The Israeli Ministry of Health ("MOH") published in April 2017 "a Digital Health Strategy" document, which sets forth the key enactments for creating a digital health support policy:

1. Regulation for the use of health data (goals, manner of use, users, transparency).
2. Regulation for the use of remote medical care (the manner in which the service is provided and service provider obligations).
3. Regulation for the access of personal electronic health record files by patients.
4. Regulation for determining the minimum content of the electronic health records.
5. Regulation applying on outcome measures of health data, which collect and monitor health data.
6. Regulation for the development and maintenance processes of clinical information systems.
7. Regulation for aspects of cyber protection of data.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The main healthcare regulations are:

- National Health Insurance Law, 5754-1994.
- Public Health Ordinance, 1940.
- Public Health Regulations (Clinical Trials in Human Subjects), 5741-1980.
- Patient's Rights Law, 5756-1996.
- Public Health Ordinance (Food) (New Version), 5743-1983.
- Protection of Privacy Law, 5741-1981 and Protection of Privacy Regulations (Data Security), 5777-2017.
- Class Actions Law, 5766-2006.

2.2 What other regulatory schemes apply to digital health and health care IT?

The General Director ("GD") of the MOH published a few circulars referring specifically to digital health, as listed below:

- GD Circular, dated 17 January 2018, regarding secondary uses of health data.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- GD Circular, dated 17 January 2018, regarding collaborations based on secondary uses of health data.
- GD Circular, dated 11 November 2019, regarding patient access to personal health data: "*Healthcare under your Control*."

The health data circulars currently prescribe the extent of protection over health data. In general, unless otherwise specified by law or approved by an explicit opt-in, any data under secondary use will be de-identified. Furthermore, any secondary use of health data for research purposes must be pre-approved by a Helsinki Committee.

2.3 What regulatory schemes apply to consumer devices in particular?

The relevant laws applying to consumer devices are:

- As of December 2019, the Medical Equipment Act, enacted in May 2012, is not yet in force. This means that there is a legal requirement to obtain marketing approval for medical devices. The MOH nonetheless operates a MAD division (medical accessories and devices), which registers and grants marketing authorisations for medical devices. On a formal level, such registration and approval is voluntary. In practice, hospitals and health maintenance organisations ("HMO") will not purchase non-approved devices. In addition, the MOH guidelines govern the process of obtaining MOH approval to import and sell medical equipment.
- The Liability for Defective Products Law, 57-401980 is a general law that imposes no fault liability for bodily injury resulting from faulty devices.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The MOH is responsible for registration and marketing approvals (see question 2.3 above), regulates the approval of clinical trials and regulates secondary use of health data.

The Privacy Protection Authority regulates maintenance of databases containing private data and privacy requirements applicable to uses of such data. The privacy protection commissioner has enforcement authority in cases of unauthorised use of data.

In general, the Authority for Law, Technology and Information (responsible for, among other things, the protection of privacy) is the entity responsible for regulating, monitoring and enforcing Israeli privacy laws, including personal data in digital databases. As mentioned above, uses of health data and collaborations involving health data are also regulated and monitored by the MOH.

The courts have jurisdiction over all issues.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

Further to what is stated in question 2.4 above, because the field is new and not comprehensively governed by Israeli legislation, it is still unclear how enforcement of legislation governing the digital health industry will evolve.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Software MADs are registered as medical accessories, e.g., CoroFlow Cardiovascular Measurement System & Accessories (software which assists in measuring flow changes in coronary arteries) as well as Insulin Insights (measurement software for diabetes patients). Other medical devices were once registered as software MADs, such as a 3D medical image processing, simulation and design software or a Neurosurgical Navigation Software.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  It is to be noted that the MOH has not yet published any guidance regarding the technologies below, creating vagueness for the entities active in the digital health field.
  - Regulation of medical practice – the issue arises when practitioners are outside the country's jurisdiction.
  - Misdiagnosis – the risk of misdiagnosis increases when medical services are provided without doctor supervision.
  - Privacy – collection, use and security standards for health data.
  - Lack of continuity in medical treatment – if a patient receives medical services from different providers, then his medical data will be scattered among different entities. This may make it more difficult to provide optimal treatment in relation to the patient's complete medical history.
- **Robotics**
  Robotic technologies are considered as emerging technologies in the field of medicine, generally used for performing human surgical/medical operations. The incorporation of new technologies, such as AI or Internet connections in robotics, enhance the performance and flexibility of this technology.
  In Israel, the company Yaskawa developed medical rehabilitation robots, which help maintain the body's quality of movement and function, rehabilitate from injuries, wounds and traumatic events and maintain daily functioning.
  XACT Robotics also developed a robot designed to perform a variety of invasive medical operations such as biopsy, ablation (catheter insertion), drainage and medication in specific areas of the body.
- **Wearables**
  Unlike other devices, wearable devices are always close to the user and thus have additional data collection capabilities (walking and pulse rate, for example). Furthermore, most wearable devices are also capable of operating without the Internet and thus the scope of data collection is greater, as is the concern of leaking sensitive information. Examples of wearable devices developed in Israel are:
  - Orcam – a wearable assistive AI device for the blind and visually impaired, that instantly reads text, recognises faces, identifies products and much more.
  - Hip-Hope of Hip-Hope Technologies – a smart wearable device, designed as a belt, worn around the user's waist. A proprietary multi-sensor system detects impending collision with the ground. Upon detection, two large-size airbags instantly inflate and protect the wearer's hips. Fall alert notifications are automatically sent to pre-defined destinations.
- **Virtual Assistants (e.g. Alexa)**
  Since virtual assistants collect a broad spectrum of data about their users, they get a more complete, accurate and

© Published and reproduced with kind permission by Global Legal Group Ltd, London

in-depth picture of the user. In view of this, the data is extremely sensitive, and any leakage may jeopardise the user's privacy, as is the case with wearables. Hence, the same general considerations apply.

- **Mobile Apps**
  Mobile apps are quite similar to wearables and virtual assistants and therefore raise similar issues. Moreover, mobile phone apps can incorporate additional hardware features (such as fingerprint, voice recognition, or various sensors) that are integrated into the mobile device.
- **Software as a Medical Device**
  This technology raises at least two main questions:
  1. Can medical device software provide medical treatment? When does provision of medical information constitute medical treatment?
  2. When is medical device software classified as a medical device, as defined in the Medical Equipment Law, 5772-2012, thereby requiring to be MAD-registered? (See question 2.3 in this regard.)
- **AI-as-a-Service**
  While systems that specialise in a particular field may support human judgment or serve as a basis for analysing a specific patient's case and determining a physician's findings, there are specialist systems that completely replace human judgment. The K system, for example, is a personalised medical information search app designed to replace medical information Internet searches that are not individually customised. The system provides relevant information according to the case, while mentioning that such information is not a diagnosis or medical advice, and that medical attention should be sought if the symptoms are severe.
- **IoT and Connected Devices**
  Please see "Wearables" above.
- **Natural Language Processing**
  NLP may be used as part of machine learning activities applied to electronic health records, whether text or audio. Usage of this technology is not regulated or standardised in Israel, and there are no instructions regarding its application in digital healthcare.

3.2 What are the key issues for digital platform providers?

- Among the various goals defined in the government's "National Digital Health Plan as a Growth Engine" is the goal to create a national digital platform for the purpose of sharing health data. However, this goal has not yet come to fruition. One of the issues in this regard is the data holders' willingness to share their data to the national central database and to agree to revenue sharing arrangements that will allow research on data originating from multiple sources.
- Problems of uniformity and standardisation also arise, since different bodies collect the data and classify the types of data stored in their databases in different ways.
- Privacy protection of the data shared through the digital platform, including its security is also a key issue.
- Obligation to present medical data to the patient (in accordance with the provisions of the GD circular on patient access to personal health data, "*Healthcare under your Control*").

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The main issues that need to be taken into account at the time of using personal data are: ownership of data; scope and nature of the independent use and sharing of the data; privacy protection of the data; revenue sharing; data use; and data sharing. See further below.

4.2 How do such considerations change depending on the nature of the entities involved?

HMOs, the entities holding most of the health data in Israel, are subject to strict regulation. For example, HMOs are limited in holding equity in start-ups and cannot invest the money generated by using health data other than for the advancement of treatment, medical service, public health or scientific research in the health field. Privacy regulations apply always, regardless of the nature of the entities.

4.3 Which key regulatory requirements apply?

In general, the manner in which health data is used is not statutorily regulated, except for regulation in connection with the protection of data privacy (Protection of Privacy Law, 5741-1981 and Protection of Privacy Regulations (Data Security) 5777-2017). The MOH has issued circulars aimed at regulating secondary use of health data (see question 2.2).

4.4 Do the regulations define the scope of data use?

Circular provisions prohibit the use of health data for purposes that do not serve the advancement of treatment, medical service, public health or scientific research in the health field. Health data should also not be used for social purposes, with an emphasis on discrimination in insurance or employment.

4.5 What are the key contractual considerations?

The main contractual issues that need to be taken into account are: ownership of data; ownership of knowhow products based on collaborations through which data is used; consideration for data sharing or knowhow products based on use of the data, such as ownership in the outside organisation (if a company is concerned); right to use the knowhow products; monetary compensation (such as royalties, licence fees, exit fees); period of use of the data; exclusivity of the data's use; reach through royalties/licences; royalty rate and stacking; and the need to use other databases.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The key area to be considered is the Protection of Privacy Law; for example, does such sharing require consent of the data subject? The general rule is that sharing/disclosure of identified

© Published and reproduced with kind permission by Global Legal Group Ltd, London

data requires informed consent, while sharing/disclosure of properly de-identified data does not.

Since use of personal health data (including de-identified data) for research is considered a "clinical trial", the necessary approvals must be obtained beforehand.

5.2 How do such considerations change depending on the nature of the entities involved?

Personal health data should also not be used for social purposes, with an emphasis on discrimination in insurance or employment.

Sharing medical data possessed by medical organisations is subject to regulation set by the MOH.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The Protection of Privacy Law, 5741-1981 prohibits the use of personal data or its delivery to another not for the purpose for which it was provided; this presumably does not apply to de-identified data.

In addition, the Protection of Privacy Regulations (Data Security) 5777-2017 states that, in the event of a contract of a database owner with an outside entity for the purpose of receiving a service, a number of provisions must be stipulated in the agreement, including; the data that the outside entity may process and the purposes of the use permitted in the contract, the manner of implementation of data security obligations the holder has, the contract term, and the return of the data to the owner at the end of the contract.

When it comes to medical data, there are specific conditions for data sharing. For example, the GD circular on secondary uses of health data states that the medical data shared for secondary use will be de-identified and sets detailed conditions for privacy, medical confidentiality and data security. Data sharing should also be done to advance the medical field. Moreover, this circular prohibits use whose social purpose is improper, with emphasis on discrimination in insurance or employment. Exclusive use of secondary health data is limited.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patent protection is governed by the Patents Law, 5727-1967. The law defines a patentable invention as one that is a product or process in any area of technology, which is novel, has inventive step and has utility and industrial application. However, the law excludes a certain type of invention: a process for human medical treatment. Diagnostic and veterinary methods are not excluded *per se*.

A discovery, scientific theory, mathematical formula, game rules and computer software *per se* are not patentable, due to case-law precedents. In general, if the invention involves a technological solution to a technological problem, it is patentable, whether the solution is in the software or not. There is no specific legislation applicable to digital health inventions, and every application is examined on its merits.

6.2 What is the scope of copyright protection?

Copyright protection is governed by the Copyright Law, 5768-2007. Copyright law protection may be particularly relevant to software and certain compilations of data, but there is no protection to databases *per se*.

As of 2018, icons, GUIs and screen presentations are not protected by copyright but rather by the Designs Law, 5777-2017. Non-registered designs are protected for three years and registered designs are protected for up to 25 years.

6.3 What is the scope of trade secret protection?

Trade secret protection is governed by the Commercial Torts Law, 5759-1999. A trade secret is defined as "business information, of all kinds, which is not in the public domain and is not easily disclosed by others lawfully and the confidentiality of which affords its owners a business advantage over their competitors, provided that its owners take reasonable steps in protecting its confidentiality". The law prohibits misappropriation of a trade secret which is defined as: (1) taking a trade secret without the owner's consent by improper means, or the use of the secret by the acquirer; (2) use of a trade secret without the consent of its owner where the use is contrary to a contractual obligation or a duty of trust the user has to the trade secret owner; and (3) acquiring a trade secret or using it without the consent of its owners, where it is clear that the trade secret has been unlawfully obtained according to (1) or (2). It should be noted that disclosure of a trade secret through reverse engineering will not, in itself, be regarded as improper. Health data is a classic example of a trade secret.

6.4 What are the typical results on academic technology transfer rules?

Israel is very active in this area and has been a world leader since the 1960s. All main academic institutions operate a tech transfer unit experienced in granting product use licenses and obtaining equity and/or royalties from commercialising products based on them. It is common practice for academic institutions to require ownership of IP generated by research conducted by the institution's researchers, subject to a license being granted to the party funding the research.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Computer software is protected by copyright, and no specific reference is made to the software of a medical device. However, copyright protects a method of expression only; thus, protection over functionality requires patent protection (see above).

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

In general, the following points should be addressed:

- the R&D phase: responsibilities of the parties, goals, deliverables, and regulatory approval process. Technical retails of access to data (whether copies will be made, or the data remotely accessed) and anonymisation thereof;
- IP: ownership and licences to background and foreground IP; responsibilities and duty to collaborate in enforcement of foreground IP; and
- arrangements for revenue sharing of commercialisation of the collaboration results: royalty bases; rate; definition

© Published and reproduced with kind permission by Global Legal Group Ltd, London

of net sales; dilution; stacking; term; milestone payments; audits; and the like.

More considerations include: exclusivity; term of the agreement; anonymisation of the data; implications of the duty to call back; and opt in *v.* opt out.

7.2 What considerations apply in agreements between health care and non-health care companies?

Agreements with public healthcare companies require special attention be given to the regulatory environment of the healthcare entity (e.g. an HMO).

- Public regulated healthcare entities are limited in their ability to hold equity in non-healthcare companies.
- Public regulated healthcare entities are restricted in their ability to accede to requests for non-compete/exclusivity arrangements.
- Healthcare organisations involved in the development of new technologies will typically consider implications on the operations, such as the duty to call back, the cost of adding a new technology to their basket of services, etc.
- In addition to access to data, healthcare organisations may serve as an alpha site for the development of new technologies.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Healthcare and academic entities, as well as companies, use machine learning in order to develop personalised, preventive, predictive and participatory medicine, including medical tools. For example, ML is used for drug repurposing or digital pathology (analysis of pathology slide images). In research performed in Israel, a deep learning algorithm trained on a linked data set of mammograms and electronic health records was found to be able to assess breast cancer at a level comparable to radiologists and to have the potential to substantially reduce missed diagnoses of breast cancer.

8.2 How is training data licensed?

There is neither specific legislation nor case law on the subject, but it seems that a licence must be obtained; as such, activity will more probably than not be considered *fair use*.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Ownership of an enhanced machine learning algorithm without human intervention may occur in respect of any of the following:

The machine, the owner of the machine, the programmer of the code, the data scientist who created the algorithm, the medical doctor who assisted in the characterisation of the algorithm.

Israeli law does not regulate the ownership of intellectual property created by machine learning, and this should be regulated in collaboration agreements. However, it is generally accepted that the company conducting the research will have the rights to the resulting products, including their intellectual property rights. It is important to note that in Israel if the invention is a method in the field of healthcare (like precision medicine), two problems arise: (1) a patent shall not be granted for a procedure for a therapeutic treatment on the human body (section 7 of the Patents Law); and (2) discovery, scientific theory, mathematical formula, game instructions, and thought processes shall be considered abstract ideas or processes of a technical nature.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Some of the main commercial considerations are:

- restrictions on the ability of the owner/possessor of the data to out-license the data (for example, due to privacy law restrictions);
- preventing misuse of licensed data (e.g. unlawful copying or unlawful disclosure to third parties); and
- remuneration to be received (fixed payment or revenue sharing of revenues received from exercising the license; in the latter case, agreeing on the royalty base may sometimes be challenging).

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

There is no specific legislation on digital health; hence, general tort law applies. This includes, primarily, the tort of negligence and the regime of strict (no fault) liability under the Defective Products Liability Law, 5740-1980. Breach of contractual warranties may also come into play.

9.2 What cross-border considerations are there?

The laws of Israel are in principle limited to its territory. However, actions conducted outside the country's borders may be subject to the jurisdiction of Israeli courts if the foreign entity collaborated with a local entity, remotely provided service to recipients located within the territory, and possibly also when damages occur or are expected to occur in Israel.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

When using cloud services, questions arise regarding the privacy and security of the data uploaded to the cloud and its security.

When the cloud is located outside of Israel, questions arise regarding the authority to transfer such data outside the country's borders. The Privacy Protection Regulations (Transfer of Personal Information to Databases Outside the State Borders), 5761-2001 set out conditions for transferring data abroad; for example, the party the data is transferred to must undertake to comply with the conditions for data retention and use applying to a database located in Israel (section 2 (4) of the Regulations).

In July 2019, the MOH authorised, for the first-time, hospitals and healthcare organisations to use cloud services. Alongside the benefits of using cloud services (such as digital medicine upgrading and cutting back on computing costs), there is concern about stealing patient medical data and the risk of cyber-attacks.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Oracle recently decided to set up a data centre in Israel, which will include two cloud servers: one designed for the government and security forces, with a particularly high level of security, and the other for the business sector, corporate clients, as well as start-ups.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

The digital healthcare market's landscape is in constant flux and there are many areas of uncertainty, not to mention that it may vary among countries. Thus, partnering with an institution with experience in the field is advantageous. Special care must be paid to the regulatory schemes applicable to both the R&D stage as well as the commercial marketing and sales stage.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

The arrival time of a large part of digital medicine technologies (such as smart apps and medical devices) is significantly short (unlike in pharma where the arrival time might take years).

The following are key factors that should also be considered:

- Maturity of the venture's product.
- Time to market (generally speaking, in digital health technologies TTM may be significantly shorter than in past traditional industries).
- Background of founders and major managers (serial entrepreneurs with proven track records are highly sought after).
- Collaboration with strategic partners (for example, having a leading HMO as a commercial partner or as the alpha site provider).
- Scope of required investment and expected return.
- Characteristics of the product's market and commercial and regulatory intellectual property challenges.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Eran Bareket holds an LL.B. degree, 1990, from Tel Aviv University and teaches in leading Israeli universities.
Eran's expertise is litigation of IP rights, unjust enrichment, competition law and complex litigations, particularly those involving issues of technology and management of multi-jurisdiction IP litigations.
Eran has vast experience appearing before all Israeli courts, including the Patents, Designs and Trademarks Registrar. He is well-versed in the fields of: IP; high technology; technology transfer and licensing; digital health; big data licensing; competition law; agency and distributorships; regulatory law (pharmaceuticals and medical devices); defence and homeland security; and governmental companies.
Eran is often involved in the Israeli Parliament (Knesset) legislative process, acting on behalf of various entities. He serves as consultant for IP matters to the Accountant General's Division of the Ministry of Finance and represents the government regarding disputes surrounding inventions by state employees (service inventions).
Eran is continuously commended by leading international guides.

Gilat, Bareket & Co., Attorneys at Law
26A Habarzel St.
Tel Aviv, 6971037
Israel

Tel: +972 3 567 2000
Email: eranb@gilatadv.co.il
URL: https://gilat-bareket.rcip.co.il/en

Alexandra Cohen holds an LL.B. degree, 2016, from Tel Aviv University.
She handles various aspects of intellectual property rights, including patents, trademarks, designs and copyrights and represents clients in litigation proceedings before Israeli courts and the Registrar of Patents, Designs and Trademarks. She also provides services with respect to commercial law as well as privacy law and regulations.
In 2016, Alexandra started her internship at Gilat, Bareket & Co. and gained experience in patents, trademarks, copyrights and commercial wrongs litigation. As of 2018, Alexandra continues her practice as a lawyer at Gilat, Bareket & Co.

Gilat, Bareket & Co., Attorneys at Law
26A Habarzel St.
Tel Aviv, 6971037
Israel

Tel: +972 3 567 2000
Email: alcohen@gilatadv.co.il
URL: https://gilat-bareket.rcip.co.il/en

Reinhold Cohn Group (RCIP) is the leading Intellectual Property consulting firm in Israel. RCIP offers a full breadth of Intellectual Property related services and expertise including protection, asset management, due diligence, and litigation & legal services. The firm operates in all areas of IP such as patents, trademarks, designs, copyrights, open source, plant breeders' rights, etc.
The group includes the patent attorneys firm, Reinhold Cohn & Partners, and the law firm, Gilat, Bareket & Co.
The synergy of patent attorneys experienced in a diverse spectrum of technological and scientific disciplines working alongside legal professionals, creates a unique and effective platform for maximising the value of a client's Intellectual Property assets by securing optimal protection.
Reinhold Cohn Group and its team of professionals are internationally renowned for excellence and continually ranked amongst the top tiers in leading international and local guides.

https://gilat-bareket.rcip.co.il/en

Gilat Bareket Attorneys at Law | Reinhold Cohn Group

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Italy


Sonia Selletti


Giulia Gregori


Claudia Pasturenzi

Astolfi e Associati, Studio Legale

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

A legal definition is not provided by Italian law: "digital health" can be defined as the use of information and communication technologies (ICT) in the health sector for the purpose of prevention, diagnosis, treatment and monitoring of diseases (in compliance with the definition provided by WHO). The term also takes on a larger significance than that of the medical-therapeutic field, including the use of lifestyle and wellness technologies.

1.2 What are the key emerging technologies in this area?

Though technological advancement occurs at a fast pace, technology applications and their use do not take place at the same speed. The factors that slow down the use of technologies in healthcare in Italy mainly concern costs related to the initial economic investment, cultural resistance of a part of the population (not necessarily the elderly, which according to some studies have shown to be able to use digital technologies for healthcare purposes), and regulatory compliance.

In Italy, the practical applications implemented to date in part or in full as regards digital health are the online sale of (non-prescription) medicinal products, the health card, the electronic medical prescription, reservations for online healthcare services (through the *Centro Unico Prenotazioni* – CUP), electronic health records, digitalised reports, telemedicine, and teleconsultation.

As for future prospects for improving patient care and rendering healthcare services more efficient, medical apps, the cloud, artificial intelligence, robotics in surgical interventions (at present primarily used in the most advanced healthcare structures) and bionics must be included. As a service, digital health insurance is remarkable.

1.3 What are the core legal issues in health care IT?

The main legal issues are: protection of privacy (please see section 4); safety; and liability for damages to the subjects involved in their use. Informed consent is even more important: the user must be properly informed in accordance with current legislation. This includes the scope of the health act, the use of innovative (digital) means and the benefits/risks that may result. The use of new healthcare IT implies requirements and training for the various subjects involved (HCPs, HCOs, supplier, producer, developer, patient, etc.), and wise liability management.

2 Regulatory

2.1 What are the core health care regulatory schemes?

In Italy, the public system for protecting citizens' health is structured around the *Servizio Sanitario Nazionale* (NHS), established with Law no. 833/1978 and inspired by the principles of universality, equality and equity in access to care as per Art. 32 of the Italian Constitution, which protects health as a "*fundamental right of the individual and an interest of the community*", and entrusted to the State and public bodies of the NHS. In one word: the State identifies the fundamental principles and determines the essential assistance levels (LEA) guaranteed as a standard throughout the country; the Regions establish health policies for local organisation and access to care. Health services are provided by the public structures of the NHS (hospitals and local health facilities), as well as by private structures duly authorised and accredited to exploit health activities with charges borne by the NHS.

Healthcare also includes the supply of medicinal products (most reimbursed by the NHS) through authorised public or private pharmacies which guarantee full coverage of the entire country, including areas at a geographical disadvantage.

This system of a public nature also leaves private operators with margins of entrepreneurial autonomy.

2.2 What other regulatory schemes apply to digital health and health care IT?

The organisation of the Italian NHS (see question 2.1) has seen a new "model" emerge in recent years, which is destined to have a significant impact on the management of healthcare in Italy: the use of new technologies in the delivery methods of patient services.

Healthcare is one of the sectors of the public administration that has seen the greatest growth in the use of new technologies,

© Published and reproduced with kind permission by Global Legal Group Ltd, London

which serves to improve the quality of care and make it more economic, efficient, and effective. While waiting for standardised regulations, the Health Authority (primarily the Ministry of Health) has issued specific guidelines such as for *Telemedicine* ("soft law" is efficient and flexible enough to "rule" fast evolving sectors).

2.3 What regulatory schemes apply to consumer devices in particular?

The wide expansion of mobile devices and apps has rapidly turned to tools for medical purposes generating *mHealth* which not only includes wellness and lifestyle apps, but also real medical-therapeutic apps.

The rapid development of technology does not go hand-in-hand with regulatory provisions, such that applicable regulatory schemes are derived from specific legislation existing at an EU and even US level in an interpretative manner.

Consumer protection legislation applies for apps in general, which provides for obligations and responsibilities of the various parties involved in the distribution chain (Legislative Decree 206/2005, the "Consumer Code"), as well as e-commerce legislation, which requires general and pre-contractual disclosures (Legislative Decree 70/2003), and the legislation on privacy EU Regulation no. 2016/679 (GDPR) and the Italian Privacy Code. Where the app falls within the definition of a medical device, the legislation on medical devices also applies (Legislative Decree 46/1997, which will be replaced by Regulation 2017/745/EU).

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The main healthcare regulatory authorities in Italy are: the *Ministry of Health*, as the promoter, implementing body, and controller of initiatives aimed at the development of digital health both at an EU and national level, through coordination that serves to guide and optimise efforts and the resources made available by all stakeholders; the *Ministry of Economy and Finance*, responsible for planning public expenditure and verifying its progress; the *Ministry of the University and Research* promoting the research; the *Privacy Authority,* as the controller of the application of the GDPR and the Privacy Code and guarantor that the processing is compliant with the fundamental rights and freedoms of individuals. Although this is not an authority with an assigned role in health IT issues, the *Ethics Committees* can play an important role with reference to projects (including clinical trials) using digital/new health technologies. In Italy the Ethics Committee may serve as a consultation body for any ethical health-related issues as well as a guarantor of the rights, safety, and well-being of the subjects involved.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The factors that may slow down the "take-off" of digital health in Italy constitute the "mirror" of the areas for intervention and improvement. The intervention areas are:

- Investment programmes to train dedicated healthcare professionals – both the new generations and the already active health workers – an increasing number of universities offer courses on the subject and continuing medical education (CME) is an important way to spread knowledge and grow culture.
- Management of the social and relationship-based aspects with patients and caregivers to reassure that the required assistance and care are ensured despite the use of new tools: this fosters efficiency and promotes quality.
- Growth of culture, and education on the use of health digital technologies to patients, caregivers, patient associations: it is important to engage in information keeping in mind that patients are increasingly "experts" and "demanding" interlocutors, while also being vulnerable subjects suffering from an illness, hence with a desire to recover.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Software as a Medical Device is ruled in Italy by Legislative Decree 46/1997 (ruling in general medical devices) and Legislative Decree 37/2010 (implantable medical devices) both enforcing EU directives. EU Regulation 2017/745 is upcoming.

As a first step it is essential to ascertain if and when a software falls within the definition of a medical device. It is advisable to be assisted by technical experts and carefully evaluate the legal profile as well: proper qualification will allow correct and effective market access.

In this regard, Italy used to refer to decisions of the EU Court of Justice which have clarified that the main criterion for classification is the intended purpose of the software. It must be used on humans for diagnosis, prevention, control, treatment, or mitigation of a disease, as well as diagnosis, control, treatment, mitigation, or compensation for an injury or handicap. The fact that the software acts directly in or on the human body is not relevant, as the EU Legislator intended to focus on the purpose of its use, and not on the effect it can produce on or in the human body (Court of Justice EU, sent. of 22 November 2012 in case C-219/2011, and sent. of 7 December 2017 in case C-329/2016).

A useful starting point exists in the EU Commission Guidelines (Meddev 2.6/6 – "*Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices*" of July 2016) and the American FDA Guidelines ("*Mobile Medical Applications – Guidance for Industry and FDA Staff*", version from 27 September 2019).

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Despite its enormous potential, telehealth encounters difficulties in finding full application in the services offered by the NHS (largely due to cultural factors, but also due to the absence of a funding model that is consistent with existing legislation). However, there is no lack of initiatives that have been launched by the public sector, supported by case law, according to which "the sole collection of data as part of a telehealth service with forwarding to the physician for review does not require authorisation, which is instead required by Italian legislation for the performance of healthcare activities" (Supreme Court, criminal section, decision no. 38585/2019).
  Telemedicine has had greater use in the private sector. This can include websites of medical offices through which patients can book visits or exams and receive results, digital

© Published and reproduced with kind permission by Global Legal Group Ltd, London

outpatient clinics, which provide the service directly at the patient's home, and insurance companies, which integrate health coverage with telemedicine services.

There are also "complex systems", some of whose functions fall within the concept of telemedicine (e.g. the artificial pancreas, a wearable that delivers insulin according to blood sugar levels through the use of an algorithm and can send glycemic data to the physician, thus serving as a telehealth system).

- **Robotics**

  The use of robots in the healthcare sector (in the surgical and rehabilitation field, implantable robotic systems, robotic pharmaceutical cabinets and "social" robots, already used in some hospitals, etc.) requires:
  - continuous software updates and maintenance to remedy malfunctions that can lead to multiple issues related to liability; and
  - protection from risks related to hacking, deactivation, or erasure of robotic memory.

  Openness to this technology requires the adequate training of health professionals as well as exhaustive information to patients, in order to comply with the rule of informed consent for the service, which is an expression of the principle of the inviolable freedom of choice of each individual.

- **Wearables**

  Examples of wearables are countless and range from fitness to medicine, from the classic pedometer and sensors for monitoring blood glucose levels, to smartwatches that perform electrocardiograms and provide warnings in the event of atrial fibrillation.

  The two main advantages are:
  - providing continuous monitoring and creating a valuable source of real life data; and
  - being able to collect data from healthy people, enabling the development of preventive medicine.

  Wearables can also be used in clinical trials, by allowing reliable or near real-time data to be obtained. By using devices that directly transfer data to researchers, the risk of transcription error is avoided and the number of visits to the research centre is reduced.

  As sensitive issues: the management of security and the protection of information collected, the qualification of certain instruments as medical devices to ensure the application of the relevant legislation.

  Additional knowledge is needed from the user and the physician, and a culture based on scientific evidence must be spread in order to gain awareness as regards actual use (a device used for recreational purposes is far different from a device to which to entrust the prevention/management of a clinical condition).

- **Virtual Assistants (e.g. Alexa)**

  The Virtual Assistant is software that interprets natural language processing and communicates with the user for the purpose of providing information or performing certain operations. In the healthcare sector there are chatbots to help users match their symptoms with an illness, and chatbots for Alzheimer's patients (to store and remind the user of information related to their life), and assistants to support women as regards fertility and menopause.

  The main issues consist of the management of the large amount of data and the liability of subjects involved in their creation and use.

  Often, these software process users' data in order to divide them into groups according to their behaviour. This activity falls within the definition of profiling, hence it is necessary to take the precautions provided for by current legislation. This also helps to prevent a violation of the principle of non-algorithmic discrimination, which requires the data controller to use appropriate profiling procedures and adopt suitable technical and organisational measures to minimise the risk of error. In this regard, the Italian Privacy Authority has adopted the 2015 Guidelines (still applicable to the extent compatible with EU Regulation no. 2016/679 (GDPR)).

  Privacy legislation applies with reference to geolocation systems, which are often used by Virtual Assistants.

- **Mobile Apps**

  There are many apps used in the health sector, which offer a wide, constantly evolving range of updated content: wellness and fitness apps; apps for time management (e.g. reminder apps); management apps (e.g. geolocation apps for services and professionals); apps for self-diagnosis and diagnosis assistance (e.g. app for measuring eyesight, app for interpreting laboratory test results), etc.

  The main problems concern the legal classification of the app (notably, whether they fall within the definition of a medical device), as well as the processing of the enormous amount of data.

  Each tool used to process personal data must be designed in compliance with current legislation according to the principle of *privacy by design*, and be set up to only process data required for each specific processing purpose.

  With reference to the app for illness management or diagnosis support, it will also be essential to provide adequate information to the patient and physician.

- **Software as a Medical Device**

  Software that falls within the definition of a medical device must comply with applicable legislation on the matter. While many different software currently fall into risk class I (affixing the CE marking without the intervention of the notified body), EU Regulation 745/2017 establishes stricter rules that may potentially lead to an increase in the risk class, with the consequent involvement of the notified body.

  The correct qualification of the software is the first step to properly approach the market: a mistake in its qualification can damage the idea. The regulatory process is equally important; it is recommended to have the support of experts and local advisors.

  Correct management of personal data and responsibilities of the manufacturer, distributors, and users are remarkable issues.

- **AI-as-a-Service**

  A regulatory assessment of the context and rules to be applied may be necessary based on the type of activity covered by the service.

  Relevant profiles include the management and processing of personal data collected and the correct identification of the subjects liable for damage resulting from system error or malfunction. The outsourcing relationship requires a specific contract to govern these profiles.

- **IoT and Connected Devices**

  One of the main problems related to IoT is the protection of privacy and the correct use of personal data collected. Risks related to the safety of devices should not be underestimated: if they are not adequately safeguarded, it can lead to multiple issues of liability in the event of malfunction.

- **Natural Language Processing**

  The difficulty of an algorithm in understanding human language is an issue. Knowledge of the meaning of each single word is not sufficient to correctly interpret a message

© Published and reproduced with kind permission by Global Legal Group Ltd, London

and can lead to contradictory and meaningless communications with the consequent risk of system unreliability.

It is necessary to develop new solutions inspired by different disciplines (e.g. linguistics, computer science, neuroscience, etc.) to understand and generate text in a natural language that is more similar to human language, and have a large amount of data to validate and implement services.

The use of NLP-based tools should be subject to a prior information to educate the user on the decoding of information received and its application in everyday life.

3.2 What are the key issues for digital platform providers?

The main issue is the liability for illegal contents uploaded to the platform.

As regards copyright, according to the Italian Court of Cassation (decision no. 7708/2019), the hosting service provider is jointly liable with the user who uploaded protected content, in the event that:

i. it is aware of the offence committed by the recipient of the service;
ii. the unlawfulness of the conduct of others is reasonably ascertainable; and
iii. it has the opportunity to take action after being informed of the illegal content uploaded.

With regard to the second point, the Court referred to the degree of diligence, saying that it is reasonable to expect from a professional network operator due to the "*technological development existing at the time that the event took place*", referring to artificial intelligence as a tool to locate illegal content uploaded to the web.

Alongside national case law is the recent decision of the EU Court of Justice issued on 3 October 2019 (in case C-18/18).

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The key issue is the processing of personal data on a big scale thanks to the use of new technologies, the Internet and virtual servers. The huge flow of information that derives from the use of digital technologies in the health sector implies the need to solve a series of issues related to the process and protection of personal data (very often of a "sensitive" nature, as it is related to health), in compliance with EU Regulation no. 2016/679 (GDPR) and Legislative Decree 196/2003 as amended by Legislative Decree 101/2018 (the "Privacy Code"), which impose compliance with more rigorous obligations and requirements than those of other sectors. An investigation by the Italian Authority for the Protection of Personal Data (www.garanteprivacy.it) carried out as part of the "*Privacy Sweep 2014*" on the most downloaded Italian and foreign medical apps from various platforms showed that the main critical issues are related to the privacy information provided to users: one out of two apps does not provide the information before installation; provides a generic disclosure; or requests excessive data with respect to the features offered.

Other issues are related to the circulation of health data, the outsourcing and delocalisation of systems and services (considering that cloud services and software on which digital health technologies are based are managed by service providers, hence the data is no longer stored on the user's physical servers, but is allocated on the systems of the supplier, which often keeps data of varying users with different or even conflicting interests and needs), as well as the storage of data in geographic locations often regulated by different legislation. These profiles are difficult to adjust at a national level, and require "*discussion at both a European and international level, in consideration of all of the implications on the processing of personal data*" (see the document of the Privacy Authority "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*" of 16 November 2011).

4.2 How do such considerations change depending on the nature of the entities involved?

The Italian law provides specific rules on the processing of health data by health professionals and health facilities (Privacy Code and Acts issued by the Privacy Authority). The Privacy Code rules information disclosed to patients by general practitioners and paediatricians (Art. 78), as well as public and private health facilities (Art. 79). Provision no. 55 of 7 March 2019 of the Privacy Authority gives indications on the privacy information scheme, the legal basis of the processing activity, the appointment of the Data Protection Officer, and processing records specifically for the processing of health-related data carried out by healthcare professionals, regardless of whether they operate as freelancers or within a public or private healthcare facility.

4.3 Which key regulatory requirements apply?

The main regulatory source is EU Regulation no. 2016/679, along with national provisions applicable to data processing activities carried out in the context of digital health. With provision no. 55/2019 above, the Privacy Authority established that the relevant processing activities "*only in a broad sense, for care, but not strictly necessary*" require, "*even if carried out by health professionals*", a legal basis other than the need to pursue the purposes of care referred to in Art. 9(2)(h), of the GDPR, "*to potentially consist of the consent of the data subject or another legal basis*". These processing activities can include those connected to medical apps if data (including health data) are collected for purposes other than telemedicine, or if these data, regardless of the purpose of the app, are accessed by subjects other than health professionals and not bound by professional secrecy. Data controllers operating in the health sector that perform various particularly complex operations (e.g. healthcare companies) shall submit the information required by the GDPR to the data subject in a *progressive* manner, providing:

- information to patients in general only as related to processing activities included in providing ordinary health services; and
- information to patients actually involved in additional processing as regards these specific activities (such as the delivery of online medical reports).

With regard to the storage period of personal data, the Privacy Authority references sector provisions that provide for the specific retention times of health-related documentation, in addition to more general rules, including Art. 2946 of the Italian Civil Code, which establishes a 10-year term for rights such as those deriving from contractual liability, among others.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

4.4 Do the regulations define the scope of data use?

A definition neither exists at a national level nor European level. The GDPR has established that the processing purposes must be specific, explicit, and legitimate. It is up to the data controller to identify the processing purpose, and specify it in the disclosure provided to the data subject (Arts 13 and 14 of the GDPR).

4.5 What are the key contractual considerations?

If a contract between the data controller and another party involves data processing on behalf of and according to the instructions of the data controller, this party must be considered a data processor. Processing activities carried out by a data processor are governed by a specific contract or other legal act in accordance with EU or Member State law, which contains the requirements provided for in Art. 28 of the GDPR. Given the special nature of tools used by digital health, the data controller must pay attention to the contractual rules carried out by the data processor, as well as the implementation by the latter of suitable technical and organisational measures provided for in Arts 32 *et seq.* of the GDPR, identifying the provider that offers suitable guarantees of compliance with privacy provisions, and in consideration that it could lose direct and effective control over its data by relying on a remote supplier. The data controller may acquire a prior declaration (supported by documents) from the supplier on the measures taken to comply with the GDPR and carry out period audits.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The identification of subjects who have access to the personal data processed and their respective roles is the main focus: in complex supply chains, it could be difficult to identify who processes the personal data involved amongst the various managers of intermediate services. It is important to establish the capacity of each subject identifying who acts as an independent data controller, who works as joint controller, and who is designated as a data processor or sub-processor for the processing activity, stipulating specific agreements that govern relations among the various subjects.

5.2 How do such considerations change depending on the nature of the entities involved?

Data sharing operations require more caution for health-related data processing as performed by healthcare professionals. The processing of such data is carried out for purposes of care, and any sharing or transfer to other subjects would need to "match" the purposes (e.g. marketing purposes). It is therefore necessary to carefully evaluate the subjects with whom the data collected are shared, and verify the purposes for which they will be processed.

5.3 Which key regulatory requirements apply when it comes to sharing data?

National provisions other than those contained in the GDPR do not exist, which, in this regard, constitutes the main regulatory reference. For the transfers of data outside the EU, in addition to the intention to carry out the transfer, the data controller must also indicate the condition of lawfulness of such transfer in the disclosure amongst those expressly provided for in Art. 44 *et seq.* of the GDPR. Such transfers are only allowed to countries that guarantee the same level of protection of personal data as provided for by legislation in Member States and, only residually, with the express consent of the data subject.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patents for inventions are governed by Legislative Decree 30/2015 (Industrial Property Code – IPC). The Code does not provide a definition for a patentable invention but outlines the scope of the patent by indicating patent requirements and the cases that remain excluded from the patentability. Patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application. The following in particular shall not be regarded as inventions: (i) discoveries, scientific theories and mathematical methods; (ii) schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers; and (iii) presentations of information. Methods for surgical or therapeutic treatment of the human or animal body and the diagnostic methods applied to the human or animal body cannot be patented.

6.2 What is the scope of copyright protection?

The term *copyright* is used to refer to the protection offered by copyright law, which in Italy is Law no. 633/1941, which gives the creator the exclusive right to use his or her work. This right lasts for the entire life of the creator, and up to 70 years after his/her death. Copyright ceases with its first sale, which means that once the creator puts a work on the market, he/she can no longer oppose the subsequent circulation of the work being sold or given to third parties, without prejudice to the prohibition on copying, duplicating, or renting it (copyright fees must be paid for these activities). According to the law, computer programs (software) and databases that, due to the choice or arrangement of the material, constitute an intellectual creation of their creator, are protected by copyright (see question 6.5).

6.3 What is the scope of trade secret protection?

Legislative Decree 63/2018 enforced the EU Directive on the protection of confidential know-how and confidential business information, expanded the protection already present in the Italian legal system in the IPC, and increased penalties for violations carried out through the use of IT tools.

What is protected are "*trade secrets*" (Art. 98 of the IPC), that is, company information and technical-industrial know-how, including commercial know-how, subject to the legitimate control of the holder. The qualification of secrecy depends on the following conditions, and namely that the information:

a) is secret, in the sense that as a whole, or in the specific configuration and combination of its elements, it is generally unknown or not easily accessible to experts and operators in the sector;
b) has economic value, given that it is secret; and
c) is subject to measures deemed reasonably adequate to keep it secret by subjects who legitimately exercise control.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

The protection is extended to data relating to tests or other secret data, the processing of which involves a considerable commitment, and whose presentation is subject to the authorisation of market placement of chemical, pharmaceutical, or agricultural products involving the use of new chemical substances.

The legitimate holder of trade secrets has the right to prohibit third parties from acquiring, revealing to third parties, or using these secrets in an abusive way without consent, unless they have been obtained independently. It is recommended to draft non-generic confidentiality agreements that explain which information must be considered secret and which is public, as well as the relative scope of dissemination. In addition to these agreements, it is advisable to think of specific organisational policies applicable to those who will access the data.

6.4 What are the typical results on academic technology transfer rules?

The technology transfer includes all of the activities underlying the passage of a series of factors (knowledge, technology, skills, manufacturing methods and services) from the field of scientific research to that of the market. This is a process that results from the collaboration between academia and industry, whose main objective is to make technology accessible to the public. As such is based on research and innovation, it is crucial to consider the protection of intellectual property, which renders the technology transfer safer and more efficient by promoting the use of the innovation by existing or newly created companies (spin-offs and start-ups). This protection usually falls under the patent protection for inventions or copyright. For inventions created in universities (or public research institutes) the reference is Art. 65 of the IPC, a provision that is not entirely clear as regards its scope and interpretation. It outlines two "scenarios". The first is of "institutional research", in which the patentable inventions made by researchers will be owned by the researchers themselves, and not by the university or public research entity. The researcher is responsible for filing the patent application and informing the institution, and the latter is granted the right to receive at least 30% of the profit of the invention in the event that it is actually exploited economically, also through the grant of licences to third parties. It is then explicitly expected that the entities can establish different ways of distributing the profit by regulatory means, which cannot reduce the benefits of the researcher below the threshold of 50% of the total. The other "scenario" concerns the so-called "funded" research, i.e. that carried out within the framework of specific research projects financed by public or private third parties, for which the entity is entitled to ownership of the invention and can clearly negotiate the rules for the use of the results with the financing party.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

In principle, software is considered a literary work of art, and is protected by copyright. In this sense, Legislative Decree 518/92 (enforcing directive 91/250/EU) expresses itself on the legal protection for computer programs, which integrated the law on copyright (Law no. 633/1941). Copyright does not protect the idea, but only its expression, and the expression of a software is in its code. Thus, copyright concerns the source code and the object code, but not their function. This means that anyone can create software with a function similar to that of the first author, as long as they do so without copying the source code and object code. The protection of copyright is automatic with the creation of the work. It is possible to register the program in the Public Software Register at the Italian Society of Authors and Publishers (SIAE) in order to obtain proof of authorship. Copyright must be governed in any software contract (development, license, transfer).

However, it cannot be excluded that a software can have a technical function, thus be assimilated to an invention, and therefore be patentable: this is possible for software as a Medical Device (SaMD). The Italian IPC (Art. 45) and the European Patent Convention (Art. 52), exclude the patentability of software "*as such*" but if it is possible to demonstrate the additional technical effect of a software, the protection deriving from the patent gains more significance because it allows the protection of the invention in any form it is reproduced, even if the patent has a shorter duration of protection (20 years) than that of copyright (70 years from the death of the creator), and requires registration in all of the areas in which protection is sought. As such, the costs are higher. Distinguishing between patentable and non-patentable software is often complicated and requires a case-by-case assessment by an expert. This is especially the case for SaMD, where the regulatory complexity of the qualification as a medical device is added to the complexity of the patent.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

In 2012, the Italian Ministry of Education, University and Research (MIUR) issued a first call for proposals for the development and strengthening of the *National Technological Clusters* to create a close link between the industrial system, research system, and national and regional institutions, in order to support strategic national lines on research, development, and training of human capital. ALISEI (Advanced Life Science in Italy) is the Life Sciences Cluster that promotes and enhances cooperation and innovation, putting online the best know-how within Italy (businesses, universities, public research entities, advanced production and high value-added services structures), acts as the driving force behind the process of transferring knowledge and technologies from the multidisciplinary research sector to the industrial pharmaceutical-biomedical sector, and serves to facilitate the attraction of public and/or private capital, which is fundamental for the development of innovative projects. The link between the various subjects of the network is generally obtained with specific agreements that may have varying legal nature, depending on the scope and purpose pursued: consortia; contractual joint ventures; partnerships between public and private entities; as well as licensing relationships if intellectual property is involved. It is recommended that a customised contractual model be prepared that is adapted for the specific project and its potential outcomes. It is crucial that the role of each party be defined in all types of agreements, and the contribution, participation methods (governance), ownership, sharing of results, as well as intellectual property and its economic exploitation.

7.2 What considerations apply in agreements between health care and non-health care companies?

The healthcare sector in Italy (as well as in the EU) is subject to strict rules to both protect health and encourage business development. Healthcare companies are structured to operate in compliance with detailed regulatory schemes, and also take part

© Published and reproduced with kind permission by Global Legal Group Ltd, London

in self-regulatory organisation that provides for the extension of rules and principles in relation to companies with less restricted activities in other sectors. It is therefore fundamental to capitalise on the experience of healthcare companies in the business and contractual model in order to encourage efficient integration and cooperation.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

AI is a matter of great interest in Italy, and also includes the Public Administration, with particular reference to the Ministry of Economy and Finance, which has recently launched a public consultation on the proposals for an Italian strategy for AI.

Digital healthcare is affected by the use of machine learning systems, which help physicians improve diagnoses, predict the spread of disease, and customise treatments. AI allows the remote monitoring of patients' health conditions (telehealth), optimisation of the management of administrative issues, and plays a fundamental role in "precision medicine", an emerging approach that takes individual variability into account in order to develop custom treatments. Through the use of smart machines that analyse a huge amount of data, it is not only possible to make early diagnoses and identify a life-saving therapy faster than traditional methods, but also allow reliable predictive medicine-based approaches. This will allow the research activity to be more effectively focused, such as the potential optimal identification of patients enrolled in clinical studies. Robotics is making a valuable contribution in operating rooms (such as tools that allow surgical intervention in a more precise and less invasive manner through the supply of maps of the parts of the body, prepared on the basis of AI algorithms, thus allowing a shorter hospital stay for patients and economic savings for healthcare facilities).

8.2 How is training data licensed?

The stipulation of a specific contract is necessary in order to obtain the training data of third parties, in which the scope of the agreement must be outlined, specifying if the ownership of the data is transferred or exclusive or non-exclusive use is granted (i.e. licence), the duration of the agreement, any right of withdrawal, rights of termination, privacy profiles that may be relevant, as well as the liability of each party. The contents of the agreement varies according to the actual needs of contractors and is based on the principle of autonomy of the parties (Art. 1322 of the Italian Civil Code), without prejudice to the principle of compliance to the law and the limitation of acts contrary to it.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Italian legislation poses some obstacles to the recognition of intellectual property rights for that created by machine learning software. The Italian Civil Code and Copyright Law (Law 633/1941) focus on the personal creation of the work, and seem to exclude the ownership of copyright by subjects other than the creator and his/her successors. At present, it appears that AI-equipped software, despite having created the work, cannot hold the consequent rights. However, even the creator (natural person) of the software may not be the owner of the rights to work created by the software, due to the lack of the requirement of personal creativity. It is evident that using this thesis potentially has negative consequences for technological development and may de-incentivise investments. An alternative route currently being explored is aimed at pre-empting the investigation of the "creative act" when programming the software. Entries of software programming would thus become central and coincide with human creativity, which is an essential requirement for the attribution of an exclusive right.

8.4 What commercial considerations apply to licensing data for use in machine learning?

One of the main issues is the identification of the criteria for the adequate financial valorisation of intangible resources, such as machine learning data. There are several criteria for estimating the value of intangible resources (e.g. the determination of creation costs and discounting of income consequent to use of the resource, the discounting of presumed royalties that the company would pay if it did not own the resource, etc.). The choice depends on the type of intangible resource, the purposes and context of the assessment, and the ease with which reliable information is found on the resource and market on which it is placed.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

To date, the model of imputation of man's indirect responsibility for any adverse outcomes produced by the use of digital health technologies has been used without any particular problems. However complex these technologies may be, the damage can always lead back to the person who planned, built, or used this tool.

This "traditional" model of imputation of liability has been questioned following the advent of the latest generation of artificial intelligence systems that operate on the basis of algorithms open to structural self-modification, determined by the experience of the system itself (machine learning), giving rise to completely unpredictable and inevitable behaviour on behalf of the person. Given this situation, a doctrine theorised the possibility of identifying the liability of the intelligent entity, whether cumulatively or independently of the liability of the programmer and/or user.

The Italian Council of State recently recognised the legitimacy of a decision by which the Public Administration ordered the transfer of civil servants on the basis of an algorithm, where there is:

- full knowledge upstream of the algorithm used and criteria applied; and
- the imputability of the decision to the entity holding power (which must verify the logic and legitimacy of the choice and results entrusted to the algorithm) (decision no. 2270/2019).

9.2 What cross-border considerations are there?

In case legal relationships may arise from the supply of the technological service such as to involve multiple subjects in different countries, thus involving multiple legal systems (such as a supplier in a country other than that of the user who uses the

© Published and reproduced with kind permission by Global Legal Group Ltd, London

technological service, but everything could be further complicated by the competing liability of third parties), in order to avoid disputes upstream as regards interpretation issues on the competent jurisdiction and applicable law in the event of dispute between the user and supplier, it is wise to pay absolute attention and precision in the regulation of contractual relations between the parties.

According to the rules of international law (Law 218/1995), EU Regulations apply (applicable only to Member States), which give priority to the rights of parties to determine the jurisdiction and the law applicable to the relationship by consensus, introducing the so-called "connection criteria" to designate the applicable jurisdiction and law only in cases where nothing has been agreed upon otherwise between the parties.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services are services offered on demand by a supplier to an end user through the Internet (e.g. data archiving, processing, or transmission).

In healthcare, cloud systems assist in innovating services provided to patients and healthcare facility management. In Italy, an example of an active cloud-based service that is subject to specific legislation (namely Prime Minister Decree 178/2015) is the Electronic Health Record (*Fascicolo Sanitario Elettronico*), through which the HCPs and patient can update, view, and share all of the health data of the latter.

The main key issues are: the outsourcing of data management, which requires appropriate rules for the control; and the need for full security guarantees of privacy.

The quality of network connectivity is essential to the efficacy of the performances and to guarantee the continuity of system accessibility. Therefore, it is essential to choose a service provider with high-quality standards in order to minimise the risks, and the cloud computing contract must cover all aspects that could represent critical or unknown factors such as to generate liability (also taking the methods to manage information and data entered in the Cloud into account).

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Non-healthcare companies must carefully know and take into consideration the healthcare sector rules and regulatory frameworks, among which, for example, are the rules:

- about the authorisation for the healthcare activity;
- about the relationships with HCPs public employees: in Italy, the performance of non-institutional assignments by public employees is subject to specific requirements (prior authorisation from the body to which it belongs is required); and
- about the marketing of compliant products: among these, not only the compliance requirements (for example, medical device standards if the medical app is qualified as such), but also the rules on information and advertising to consumers.

The evaluation of the legal environment is crucial to support the business model.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

Once again, the knowledge of the legal framework is crucial for each choice functional to an investment, in order to identify the strengths and possible critical points of the project.

The evaluation requires an interdisciplinary approach, hence it is advisable to have a highly specialised and differentiated team that is constantly updated. On this point, given that the digital sector evolves on a continuous basis, we must consider the issue of obsolescence, which characterises the digital sector, which, in comparison to others, is in constant evolution.

Market needs must then be analysed, while considering that the two main trends in the health sector consist of, on one hand, unmet medical needs and, on the other hand, sustainability of the health system.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Sonia Selletti graduated in law, University of Pavia, 1991. Admitted 1994, Milan. Supreme Court Barrister.
After practising international law and after a period as head of the internal legal office of an Italian pharmaceutical company, in 1995, Sonia joined Astolfi e Associati where she is Partner, Head of the Life Sciences Group. She gained 25 years of expertise in pharmaceutical and health legislation for medicinal products, cosmetics, medical devices and health supplements.
Sonia is a member of the Supervisory Bodies in sanitary and pharmaceutical companies pursuant to Legislative Decree 231/2001 aimed at preventing criminal liabilities of corporate entities.
She is the director responsible for the specialist legal journal *Rassegna di diritto farmaceutico e della Salute*. She has authored various publications on legal topics concerning Life Sciences. She is co-author of "e-patient e social media", *Il Pensiero Scientifico Editore*, 2016.
Sonia collaborates with the University of Pavia in administrative law courses on procedures for the access of medicines to the market. She also provides training courses in the healthcare and pharmaceutical field at CME events for health professionals.

Astolfi e Associati, Studio Legale
Via Larga, 8
20122 Milano
Italy

Tel: +39 02 885561
Email: sonia.selletti@studiolegaleastolfi.it
URL: www.studiolegaleastolfi.it

Giulia Gregori graduated in law, University of Pavia, 2011. She has been a member of the Milan Bar Association since 2019.
Giulia has been working with the Astolfi e Associati law firm since 2013 where she mainly works in the field of pharmaceutical and healthcare law. She has also gained experience in data protection law.
She is editorial assistant and member of the editorial board for the specialist legal journal *Rassegna di diritto farmaceutico e della salute*, as well as the author of several publications.

Astolfi e Associati, Studio Legale
Via Larga, 8
20122 Milano
Italy

Tel: +39 02 885561
Email: giulia.gregori@studiolegaleastolfi.it
URL: www.studiolegaleastolfi.it

Claudia Pasturenzi graduated in law, University of Pavia, 2010. She has been a member of the Pavia Bar Association since 2014.
Claudia has been working with Astolfi e Associati since 2014 and mainly works in the field of pharmaceutical and healthcare law, in handling questions on the advertising of medicinal products and medical devices, also with regard to new communication channels (social media).
She is a member of the editorial board for the specialist legal journal *Rassegna di diritto farmaceutico e della salute*, as well as the author of several publications.

Astolfi e Associati, Studio Legale
Via Larga, 8
20122 Milano
Italy

Tel: +39 02 885561
Email: claudia.pasturenzi@studiolegaleastolfi.it
URL: www.studiolegaleastolfi.it

Astolfi e Associati, Studio Legale was founded by Antonio Astolfi in 1955. Fostering his original interest in international trade law, he founded the law journal *Diritto Comunitario e Degli Scambi Internazionali* (*EU Law and International Trade Law*). Later, in the sixties, he developed a strong interest in pharmaceutical and health law (life sciences) showing longsighted vision. In 1968, he founded the law journal *Rassegna di Diritto Farmaceutico* (*Pharmaceutical Law*), still edited today after more than 40 years, in its new version *Rassegna di Diritto Farmaceutico e Della Salute*. This heritage is today the practice area of Astolfi e Associati, deployed from civil, labour, commercial and banking law to pharmaceutical, health and food law, proposing complementary and comprehensive services to clients to fully meet their needs for legal advice. Astolfi e Associati advise Italian and foreign clients in both extrajudicial and judicial matters.

www.studiolegaleastolfi.it

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Japan


Kazunari Toda


Mia Gotanda

GVA Law Office

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no clear definition of "Digital Health". In general, digital health includes applications, systems, and services related to medical care and health which broadly utilise digital techniques and data.

Specifically, "Digital Health" includes: 1) medical systems (electronic health record systems, systems to establish linkage within the hospital and externally, solutions to assist medical office work, etc.); 2) remote treatment systems (remote medical treatment systems, teleconsultation systems, etc.); 3) disease prevention medical systems (applications to prevent specified disease, healthcare applications, etc.); 4) medical devices (digital treatment applications, sensing devices, wearable devices, etc.); 5) diagnosis support systems (software supporting AI image diagnostic systems, software to indicate disease progression and others); 6) big data (medical, nursing, etc.); and other businesses.

1.2 What are the key emerging technologies in this area?

Although there are a variety of cutting-edge technologies which are expected to be put to practical use in the near future, technology using AI is being paid particular attention. There are many systems which utilise AI technology that include medical applications, image diagnosis supporting systems, mental health tech, medical interview systems, and others.

1.3 What are the core legal issues in health care IT?

If healthcare IT falls under "medical device" defined in the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices, then it is subject to the Act for manufacture and sales. In addition, the Act on the Protection of Personal Information will also be applied to the use of personal information.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The core regulation applied to healthcare business is the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices. If the product falls under "medical device" as defined in the Act, it is necessary to obtain approval of the product and license for manufacture and sales. The term "medical device" is defined as "appliances or instruments, etc. which are intended for use in the diagnosis, treatment or prevention of disease in humans or animals, or intended to affect the structure or functioning of the bodies of humans or animals (excluding regenerative medicine products), and which are specified by Cabinet Order". Medical devices are classified into four classes, depending on the risks to human or animal. The approvals and licenses also differ depending on each class.

Advertisement for medical devices that contain misleading information, etc. is prohibited. If approval as a medical device is not granted to a device, then advertisement containing medical efficacy, effects or performance is strongly prohibited.

2.2 What other regulatory schemes apply to digital health and health care IT?

How to handle personal information becomes an issue in much of digital health and healthcare IT. Sections 4 and 5 below describe the overview of the Act on the Protection of Personal Information.

In addition, the following various regulations may be applied, depending on the type of business:

- Medical Practitioners Act (telediagnosis, gene testing, etc.).
- Medical Care Act (establishment of healthcare corporation).
- Pharmacists Act (remote medicine prescription).
- Act on Utilisation of Telecommunications Technology in Document Preservation, conducted by private business operators, etc. (electronic medical record).
- Act on Regenerative Medicine.
- Clinical Trials Act.
- Insurance Laws.
- Product Liability Act.

2.3 What regulatory schemes apply to consumer devices in particular?

According to the Consumer Contract Act, notwithstanding the clauses provided in the contract, if consumers suffer a disadvantage as a result of certain clauses (including but not limited to the following clauses), such clauses will be null and void:

1) clauses that completely exempt a trader from liability to compensate a consumer for damage;
2) clauses that partially exempt a trader from liability to compensate a consumer for damage arising from an intentional act or gross negligence of the trader; or

© Published and reproduced with kind permission by Global Legal Group Ltd, London

3) clauses that force the consumer to waive the right to cancel the contract if the trader defaults.

According to the Act on Specified Commercial Transactions, in the case of mail-order sales (including sales via internet), a company shall indicate the prescribed items, such as the price, the timing and method of payment, the timing of the delivery, information concerning the withdrawal or the cancellation, the name, address, and telephone number of the seller or the service provider, the liability in case the goods have a hidden defect, and the computer specifications, etc.

The Act against Unjustifiable Premiums and Misleading Representations prohibits representations which mislead consumers in terms of quality, terms and conditions, etc.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The Ministry of Health, Labour and Welfare exercises jurisdiction over medical devices (for humans). The Ministry entrusts the Pharmaceuticals and Medical Devices Agency (PMDA) to conduct investigations for approvals; licence to manufacture and to conduct the sale of a medical device must be made via the prefectural governor of the region.

The Act on the Protection of Personal Information is under the jurisdiction of the Personal Information Protection Committee, and the Consumer Affairs Agency has jurisdiction over the Act on Specified Commercial Transactions, the Act against Unjustifiable Premiums and Misleading Representations and the Consumer Contract Act.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

If any individual or entity manufactures or conducts sales of a medical device without obtaining a licence to do so, the individual or entity shall be subject to imprisonment for not more than three years, or a fine of not more than 3,000,000 JPY.

Any false or exaggerated advertising made by an individual or entity is subject to imprisonment for not more than two years, or a fine of not more than 2,000,000 JPY and, in addition, the individual or entity who committed the violation is charged with 4.5% of the sales amount of products sold for the period when such individual or entity was engaged in the illegal activities (except when the fine is 2,250,000 JPY or less).

Further, the individual or entity shall be subject to imprisonment for not more than two years or a fine of not more than 2,000,000 JPY, if such individual or entity makes an advertisement for a medical device before or without obtaining approval for such medical device.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Software as a medical device requires approval from the national government if it falls under "medical device". The definition of a medical device is given in question 2.1 above. In addition, the applicability of a Medical Device Program shall be determined by considering the overall risks including the following factors: 1) how much does the program contribute to the treatment and the diagnosis of diseases by considering the importance of the results obtained from such program; and 2) the probability of the total risks, including the risks to human life and health in the case where a system failure occurs to the program.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  A medical practice licence is required to provide remote services using IT tools if such service is considered as "medical practice". Diagnosis and treatment are considered as "medical practice", but the provision of general information is not considered as "medical practice". Interpretation of "medical practice" is made on a case-by-case basis by referring to previous cases as examples.
  If the service falls under "medical practice" and such service is provided by a medical practitioner (doctor), the propriety of such remote medical treatment becomes an issue because Article 20 of the Medical Practitioners Act requires doctors (in principle) to give a face-to-face diagnosis. However, as the necessity of remote medical treatment grows, the Ministry of Health, Labour and Welfare issued the "Guideline for online diagnostics", and the guideline states that if a doctor gives medical treatments by following the guideline, it does not constitute a violation of the Act.
- **Robotics**
  If a robot falls under "medical device", then it is subjected to the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals. It is likely that the manufacturer shall bear product liability or tort liability in the event of a malfunction in the robot.
- **Wearables**
  With regards to wearable terminals, it is whether or not 1) the wearable terminal measures and collects data, and 2) the program that analyses collected measurement data falls under "medical device", that issues start to arise.
  Question 2.1 above describes the definition of "medical device", and question 2.6 describes the applicability of software as "medical device".
  For example, with regards to item (1), a program using a portable device with built-in sensor to detect body motion is not deemed to be a "medical device", however, a thermometer, hemo piezometer, and cardiac electrogram are considered as "medical devices". Whether or not a wearable terminal is a medical device is dependent on the information to be measured or collected.
  With regards to item (2), a program which merely displays, transfers, and stores measurement data of an individual's health status only for health promotion, is not considered as a "medical device".
- **Virtual Assistants (e.g. Alexa)**
  Virtual Assistants are considered as mere supplementary tools to doctors; therefore, in general, it does not conflict with the Medical Practitioners Act.
  However, if the function of such supplementary tools falls under the definition of a "medical device" in light of applicability as a Medical Device Program as described in question 2.6 above, then they are subject to laws and regulations.
- **Mobile Apps**
  If they fall under the definition of a "medical device", in light of applicability as a Medical Device Program as described in question 2.6 above, then they are subject to laws and regulations.
- **Software as a Medical Device**
  If they fall under the definition of a "medical device", in light of applicability as a Medical Device Program as

© Published and reproduced with kind permission by Global Legal Group Ltd, London

described in question 2.6 above, then they are subject to laws and regulations. Almost the same as "Mobile Apps".

- **AI-as-a-Service**
  At the current technical level, AI is not considered to be eligible to make definitive conclusions concerning patients' diseases and it is considered as a supplementary tool to physician service. According to such consideration, a medical practitioner shall be responsible for making the definitive conclusion about patient's diseases so that AI shall not conflict with the medical practitioner licence as prescribed by the Medical Practitioners Act.
  Applicability of AI medical devices as a "medical device" shall be considered in light of criteria of applicability as a Medical Device Program as described in question 2.6 above. Refer to section 8 for more information about AI.
- **IoT and Connected Devices**
  Similar to Robotics and Wearables, the applicability of "medical device" and product liability will apply to IoT and Connected Devices.
- **Natural Language Processing**
  There are no special legal regulations specified for Natural Language Processing. Refer to section 8 for details.

3.2 What are the key issues for digital platform providers?

A provider of a digital platform in digital health would generally need to obtain personal information and sensitive information (special care-required personal information) in most cases. Special attention should be paid to the Act on the Protection of Personal Information.

The Act on Anonymised Medical Data That Are Meant to Contribute to Research and Development in the Medical Field, was established in 2017, and it is expected that this Act will facilitate the use of big data in the medical field. In other words, it became possible for medical institutions to provide authorised operators with the medical information of patients by following opt-out procedures, and authorised operators may create anonymously processed information and provide the information to those who are interested in the information.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

If the information to be used falls under "Personal Information" prescribed by the Act on the Protection of Personal Information, then acquiring, utilising and providing such information is subject to the Act. Further, if the information falls under sensitive information (special care-required personal information), it is subject to more rigid control.

In the Act on the Protection of Personal Information which applies to private business operators, "Personal information" is defined as "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual) or as "information that contains an individual identification code". An "individual identification code" includes (but is not limited to) DNA information, physical traits, and passport number of the individual.

Special care-required personal information on health includes an individual's medical history, disabilities, the results of a medical check, and the fact that the individual receives guidance, diagnosis and dispensing of diseases and genome information obtained from a gene test.

Anonymously processed information has high flexibility for use compared to general personal information, however, certain provisions shall be applied to the process and record.

4.2 How do such considerations change depending on the nature of the entities involved?

The handling of personal information by a central government organisation, local government and incorporated administrative agencies, is regulated by separate laws to those applied to private business operators.

In addition to the Act on the Protection of Personal Information, guidelines are provided by the government for medical institutions, gene data businesses, medical information system providers, and telemedicine.

4.3 Which key regulatory requirements apply?

To handle personal information, it is required to specify the purpose of utilising personal information as explicitly as possible. To acquire sensitive information (special care-required personal information), it is, in principle, required to obtain the consent of the principal.

Refer to section 5 for regulation on providing personal information to a third party.

4.4 Do the regulations define the scope of data use?

Personal information shall not be handled beyond the necessary scope as to achieve its specified utilisation purpose prescribed at the time of obtaining such information.

4.5 What are the key contractual considerations?

The key contractual considerations that should be included in a contract are the scope of target data, authorisation to use the data and generated data, remuneration and payment, warranty, and ownership of intellectual property rights, etc.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

If the information falls under "Personal Information" as defined under the Act on the Protection of Personal Information, providing such information to a third party should be subject to the Act. Further, if the information falls under sensitive information (special care-required personal information), then it is subject to more rigid control.

Refer to question 4.1 about definitions of "Personal Information" and "special care-required personal information" and question 3.2 for the Act on Anonymised Medical Data That Are Meant to Contribute to Research and Development in the Medical Field.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

5.2 How do such considerations change depending on the nature of the entities involved?

Same as question 4.2.

5.3 Which key regulatory requirements apply when it comes to sharing data?

To provide personal information to a third party, in principle, each of the following is required: 1) the consent of the principal; 2) opt-out procedures by submitting an application to the Personal Information Protection Commission; 3) providing personal information accompanied by the entrustment of handling the personal information; and 4) for joint use with a specified person and indication of necessary information about such joint use. However, it is not allowed to provide special care-required personal information to a third party by following opt-out procedures.

Further, it is required in principle to obtain the consent of the principal for providing the personal information to a third party who is outside Japan.

6 Intellectual Property

6.1 What is the scope of patent protection?

"Invention" may be protected by the patent rights under the Patent Act. The term "Invention" is defined as a highly advanced creation of technical ideas utilising the laws of nature.

An invention can be registered as a patent if a patent application is submitted to the patent office, and the patent office acknowledges its industrial applicability, novelty, inventive step and earliest application, and it is not contrary to public order and morality.

In the digital health field, it is assumed that hardware or a program of medical or healthcare devices may be accepted as a patent.

A patent right comes into effect when registered and the term of a patent right expires after a period of 20 years from the filing date of the patent application.

6.2 What is the scope of copyright protection?

"Work" protected by the Copyright Act means a creatively produced expression of thoughts or sentiments that fall within the literary, academic, artistic, or musical domain.

Unlike patent right, no procedures or registration is necessary for copyright, and copyright becomes effective at the time of creation.

In the digital health field, it is assumed that software, programs, text, pictures, and images are subject to copyright.

Also, a database may be recognised as work protected by copyright if the database contains creativity on the selection or systematic construction of information. However, a database is not recognised as work protected by copyright if the database merely contains information constructed mechanically.

A copyright owner (author or its successor) is authorised to exercise the copyright, including but not limited to the right of reproduction, right of transfer, right to transmit to the public and right of adaptation, and the third party shall not copy, transfer, transmit to the public, or adapt the work without the consent of the copyright owner.

In principle, copyrights commence at the time of the creation of the work and end 70 years after the death of the author.

6.3 What is the scope of trade secret protection?

The term "trade secret", protected by the Unfair Competition Prevention Act, means technical or business information useful for business activities, such as manufacturing or marketing methods, that are kept secret and are not publicly known.

In particular, the requirements of a "kept secret", is subject to the structure, including information management rules within the organisation or clarification of information medium, which need to be disclosed to employees to objectively recognise that such trade secret is "kept secret". The improper acquisition, disclosure and use of trade secrets is illegal.

6.4 What are the typical results on academic technology transfer rules?

The question of intellectual property rights deriving from research that has been conducted at a university, and whether the ownership belongs to the university or the individual researcher, depends on the operation conducted by each university. Unlike a company, it is not always the case that all intellectual property rights created at the university will belong to the entities: the rights may belong to students who participated in the research. Therefore, it is necessary to confirm who owns the intellectual property rights for each project before concluding any contracts.

Patent rights shared among university and private companies through joint research may, in principle, be used or commercialised by each party. However, because universities rarely use its own patent right for commercial use, the university often requests the company to pay the university a part of the profits from the commercialisation of the patent by the company (called as non-exercising compensation). Further, it is important to set the condition for publication as to the timing of the presentation by the university and the patent application by the company.

For an entity (contractor) to hold 100% ownership of the intellectual property rights derived from research and development project, of which the funding is contributed by the national government, the following are the requirements that a contractor needs to agree to under its contractual obligations as prescribed under Article 19 of the Industrial Technology Enhancement Act:

1) in cases where the result of specified research and development is obtained, the contractor will make a report to that effect to the national government without delay;
2) in cases where the national government finds it particularly necessary for the public interest and makes a request, making clear the reasons therefor, the contractor will grant the national government the right to use said intellectual property without charge;
3) in cases where the national government recognises that the contractor has not utilised said IP for a considerable period of time and does not find any justifiable grounds for it, and when the national government finds it particularly necessary for promoting the utilisation of said IP and makes a request, making clear the reasons therefor, the contractor will grant a third party the right to use said intellectual property; and
4) in cases where it intends to transfer said intellectual property, or give consent to the establishment for the transfer of the right to use said intellectual property specified by Cabinet Order, the contractor will receive the approval of the national government in advance, except in cases where the said intellectual property is transferred as a result of a merger or a split, or in cases specified by Cabinet Order as being unlikely to hinder the utilisation of said intellectual property.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Software is protected under the Copyright Act as the work of a program. Software with novelty and inventive step may also be protected as a patent right.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

When multiple companies jointly operate a digital health business, it is important to regulate in the contract, factors such as (but not limited to) ownership of intellectual property rights, cost-sharing, profit-sharing, and division responsibility, such as the role for development, sales and customer service.

7.2 What considerations apply in agreements between health care and non-health care companies?

Manufacture and sale of products which fall under "medical device" prescribed by the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices can also be performed by the company which has obtained a licence from the national government.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Typically, AI automatic diagnosis systems equipped with a machine learning function continuously improve the accuracy of diagnosis by AI.

In light of the above, where the performance of the medical device has been improved by machine learning, and approval has been granted by the government, additional approval may not be required for such improvements in the program, if the government has in advance acknowledged the plan of such changes in performance of the program.

8.2 How is training data licensed?

Licence is granted through the execution of contracts.

Training data is rarely protected as under copyright or trade secret, as it is normally not protected by any specific laws. As such, in principle, any person who can access the data can freely use the data. Therefore, it is necessary to stipulate conditions of use in the contract.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Copyright and patent right of an original algorithm, which was created by a person without utilising machine learning, belongs to the creator, in principle.

In principle, no one has any legal intellectual property right for the newly created algorithm from machine learning, except for the parts which include characteristics of an original algorithm, because creation by machine is not subject to the intellectual property laws.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The scope of target data, authorisation to use the data and generated data, remuneration and payment, warranty, ownership of intellectual property rights, shall be specified in the contract.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

A person who provides a product or service in connection with digital health to users shall be responsible for compensation for damage to users caused by a defect of such product or service.

In the event damage is suffered by the user due to a defect of the product, the manufacturer of such product may be responsible for compensation for damage to users as product liability.

In the event that a doctor makes a wrong diagnosis of someone's illness by using an AI program and the patient suffers damage, the doctor shall be responsible for the damage, as the AI program is just providing assistance to the doctor's judgment.

9.2 What cross-border considerations are there?

In principle, the liability under the contract is subject to the governing terms stipulated in the contract.

However, contracts with individual consumers, tort, and product liability may be governed by the applicable law of the place of residence of the consumer or the place where the damage has occurred, regardless of governing law agreed in the contract.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

In the case where a business operator stores users' personal information on a cloud service provided by a third party, consideration shall be given to whether the storage is subject to the provision of personal information to the third party under the Act on the Protection of Personal Information.

The government states that the storage is not subject to the provision of personal data to a third party and it is not necessary to obtain the consent of the principal if the provider of the cloud service never handles any personal information stored by its customer (e.g. specified in the contract).

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

The important issue for non-healthcare companies is whether or not the products and services need approval as a "medical device". If a company wishes to conduct business for the medical device, considerable cost and term would be expected for the approval and licence.

There are many stakeholders in the healthcare business, including the national government, local governments, medical institutions, the health insurance society and others; thus, consultation or alliance with such relevant entities may be needed in many cases.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

As compared to other business, the healthcare business, especially for business related to a medical device which requires a licence from the national government, tends to have a long period for development and obtaining approval, which can be costly. Therefore, it is difficult to have a return on investment in a short period of time. Moreover, the healthcare business involves human life and bodies, so stricter regulations are applied and it requires cautious business management.

Nevertheless, digital health business does not require great care and requires less development cost as compared to the ordinary medical device business. Digital health business has high social needs so it can be said that the digital health business is one of the most valuable investment opportunities in Japan from a mid- to long-term perspective.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Kazunari Toda is a partner at GVA Law Office. He has experience in various fields of law, from litigation, intellectual property to corporate governance. Since joining GVA Law office in 2016, he has expanded his experience, focusing on cross-border transactions, in particular in the Information Technology Industry. His fields of expertise are international legal affairs, corporate affairs, and mergers and acquisitions (M&A). However, his passion lies in the HealthTech industry. He graduated from Seijo University with a Bachelor of Law and received his Juris Doctor from Waseda Law School. Mr Toda is fluent in both Japanese and English.

GVA Law Office
EBS Building 3F
1-7-7 Ebisunishi
Shibuya
Tokyo
Japan

Tel: +81 3 6712 7525
Email: k.toda@gvalaw.jp
URL: www.gvalaw.jp/en

Mia Gotanda joined GVA Law Office in 2018. Before joining the firm she worked as an in-house legal counsel with a medical device company where she acquired her interest in HealthTech. Her fields of expertise are mergers and acquisitions (M&A), corporate affairs and IT legal affairs. She has provided much legal support in cross-border transactions during her tenure as a practising attorney and in-house counsel. She received her Bachelor of Law and Juris Doctor from Nihon University and Rikkyo University Law School respectively.

GVA Law Office
EBS Building 3F
1-7-7 Ebisunishi
Shibuya
Tokyo
Japan

Tel: +81 3 6712 7525
Email: m.gotanda@gvalaw.jp
URL: www.gvalaw.jp/en

GVA Law Office's management principle is to provide business infrastructure that goes beyond providing legal services, to challengers worldwide. Since our establishment, we continuously assist our clients by building, developing and facilitating business expansion, particularly for IT-related companies. Our firm provides legal solutions for businesses outside the common IT industry and our legal services span all fields necessary for a business venture, from start-up to IPO. We specialise in cutting-edge industries such as FinTech, HealthTech, AI, Blockchain and DeepTech. At GVA Law Office, our professionals have the drive and knowledge to support domestic and overseas business expansion, and cutting-edge companies of any type and phase. Our head office is located in Tokyo and is supported by the China Desk and the Malaysia desk. We are actively expanding our service to the South East Asia region and have established offices in Thailand and the Philippines.

www.gvalaw.jp/en

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Kenya


John M. Ohaga


Stephen Mallowah


Catherine Kariuki


Janet Othero

TripleOKLaw LLP Advocates

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

In Kenya, digital health is synonymously used with the term **eHealth** which finds its place in legislation, i.e. the Health Act of 2017, and which is defined as "the combined use of electronic communications and information technology in the health sector including telemedicine".

1.2 What are the key emerging technologies in this area?

The key emerging technologies in digital health are:

Telehealth: The use of telecommunications and virtual technology to deliver healthcare outside of traditional healthcare facilities.

Telemedicine: The remote delivery of healthcare services over telecommunication infrastructure e.g. video conferencing. The Kenyan government in May 2015 launched a first phase of a national telemedicine initiative for the poor and the marginalised as one of the programmes that will help to tackle non-communicable diseases.

Mobile health (**mHealth**): Involves delivering medical services using mobile technologies. In 2013, Kenya's Mobile Post Exposure Prophylaxis (**mPEP**) initiative was developed through a public-private partnership initiative with mHealth Kenya and the Centre for Disease Control and Prevention Foundation (**CDC**).

Integrated Hospital Management Information System (**HMIS**): Is an element of health informatics that focuses mainly on the administrational needs of hospitals.

1.3 What are the core legal issues in health care IT?

The following are the core issues that affect healthcare IT:

- **Protection of data regarding the health status of an individual by the Data Protection Act**: The health status of an individual falls squarely within two classes of data as envisioned by the Data Protection Act, 2019 (**DPA**). The first is the definition of "sensitive personal data" which has been defined as data revealing the natural person's health status, genetic data of the data subject amongst other components. The second is "health data" which is data related to the state of physical or mental health of the data subject.

  The DPA provides guidance regarding the processing of personal data relating to health. Notably, personal data relating to the health of a data subject may only be processed by or under the responsibility of a healthcare provider; or by a person subject to the obligation of professional secrecy under any law.
- **The duties of the data controller and data processor under the DPA**: Section 18 of the DPA, states that bodies designated as data controllers and data processors must register with the Office of the Data Commissioner. The DPA imposes several obligations on processors and controllers. Including registration with the data commissioner, duties corresponding to data subjects' rights, etc.
- **Profiling and automated processing of health data**: Section 35 of the DPA states that every data subject has a right not to be subject to a decision based solely on automated processing, including profiling which produces legal effects or significantly affects the data subject. This binds healthcare IT providers as they contract with data subjects.
- **The prioritisation of data regarding HIV Patients as outlined under the HIV/AIDS Prevention and Control Act, 2006**: The Act necessitates technology providers who intend to store and analyse data regarding HIV patients to accordingly create robust digital frameworks which use encryption and pseudonymisation techniques to further protect the identities of such data subjects.
- **Prohibited disclosure of information in respect of HIV/AIDS Patients under the HIV and AIDS Prevention and Control Act, 2006**: Under Section 22 of the Act, persons in possession of any information regarding the result of a HIV test or any related assessments to any other person are expressly prohibited from disclosing that information, except through numerous exemptions identified therein.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The Constitution of Kenya, 2010

Access to healthcare is a fundamental right and freedom enshrined under Article 43 (1) (a) of the Constitution providing in part that "every person has the right to the highest attainable standard of health, which includes the right to healthcare services…". The integration of digital healthcare into the health sector contributes towards achieving this standard. Article 31 also guarantees the right to privacy for all citizens in relation to their personal information.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Health Act, 2017
This Act aims to regulate health products and health technologies. Section 104 of the Act provides that within three years from the operation of the Act, the Cabinet Secretary responsible for healthcare shall ensure the enactment of legislation that provides for the collection and use of personal health information, management of disclosure of personal health information, protection of privacy, health service delivery through M-Health, E-learning and telemedicine, E-waste disposal and health tourism.

In addition, Sections 103–105 of the Health Act protects and regulates the use of eHealth in the collection, retrieval, processing, storage, use and disclosure of personal health information.

Public Health Officers (Training, Registration and Licensing), 2013
This Act provides for the training, registration and licensing of public health officers and public health technicians.

Mental Health Act
This Act amended and consolidated the law relating to the care of persons suffering from mental disorders, or mental sub-normality with a mental disorder, for the custody of these persons, management of their properties, management and control of a mental hospital and for custodial purposes.

HIV and AIDS Prevention and Control Act 2006
This Act is designed to provide measures for the prevention, management and control of HIV and AIDS, to provide for the protection and promotion of public health and for the appropriate treatment, counselling, support and care of persons infected or at risk of HIV/AIDS.

2.2 What other regulatory schemes apply to digital health and health care IT?

The other regulatory schemes that apply are:

Health Records and Information Managers Act, 2016
The Act provides for the training, registration and licensing of the health records and information managers. It provides for the establishment, powers and functions of the Health Records and Information Managers Board.

Kenya Information and Communication Act, 2009
The Act provides for the establishment of the Communications Authority of Kenya whose mandate is to license and regulate postal, information and communication services in accordance with the Act.

Access to Information Act, 2016
The Act gives effect to Article 35(1) of the Constitution which states that "Every citizen has the right of access to: (a) information held by the State; and (b) information held by another person and required for the exercise or protection of any right or fundamental freedom". This enables individuals to access their medical records that are held in any medical institution.

Data Protection Act
Section 46 of the Act addresses personal data relating to health and provides that personal data relating to health of a data subject may only be processed: (a) by or under the responsibility of a healthcare provider; or (b) by a person subject to the obligation of professional secrecy under any law.

2.3 What regulatory schemes apply to consumer devices in particular?

The following laws govern the standards and quality of consumer devices in Kenya:

Consumer Protection Act, 2012
The Act provides for the protection of the consumers and prevents unfair trade practices in consumer transactions. Section 5 of the Act provides for the supplier of goods and services warranting that they are of a reasonable merchantable quality. The same is provided for under the Sale of Goods Act Section 16.

Standards Act
The Act promotes and provides the standardisation of the specification of commodities.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The following lists the principal regulatory authorities:

The Ministry of Health
Section 15 of the Health Act mandates the Ministry of Health to formulate health policy and regulation, provide national referral health facilities, capacity building and provide technical assistance to counties.

Kenya Bureau of Standards
It is established under Section 3 of the Standards Act and is mandated to inspect imports based on standards required by the Act.

The Consumer Protection Committee
The Committee is established under Section 89 of the Consumer Protection Act 2012 and part of its function is to include formulating policies relating to the Act in the interest of consumers, promotion or participation in consumer education and providing advice to consumers on their rights and responsibilities regarding the law.

Kenya Medical Supplies Authority (KEMSA)
This is a state corporation under the Ministry of Health established under the KEMSA Act 2013 whose mandate includes to procure, warehouse and distribute drugs and medical supplies for prescribed public health programmes, the national strategic stock reserve, prescribed essential health packages and national referral hospitals.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The following are the key areas of enforcement in digital health and healthcare IT:

1. Patient management in the case of patients with chronic diseases where the specific interface to be used will need to be built around patients and their need for effectiveness.
2. Data collection of patient details and reporting on their progress.
3. Administration/management of different healthcare.
4. Stock and supplies management in hospitals.
5. Service delivery (vaccines, family planning, maternal and childcare, HIV treatment and support).
6. Clinical decision support and alerts.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

The following regulations apply to Software as a Medical Device and its approval for clinical use:

1. **The Pharmacy and Poisons Act, Cap 244 (2002) and the Guidelines on Submission of Documentation for Registration of Medical Devices**
   The Kenya Pharmacy and Poisons Board supervises medical device regulation. Under the guidelines, a medical device means among others, **software** or any other similar or related article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific defined purposes.
2. **The KEBS Guidelines for Inspection of Imported Medical Devices, Food Supplements, Medical Cosmetics, Herbal Products and Other Borderline Products** provides that importers have to apply for Pre-Export Verification of Conformity as the first step of initiating importation of any medical devices in order to obtain Certificates of Conformity from KEBS.
3. **Global Harmonisation Task Force for Medical Devices Guidance Documents**
   This task force encourages a convergence in standards and regulatory practices related to the safety, performance and quality of medical devices. It provides publications of harmonised guidance documents for basic regulatory practices.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Licensure: The legal requirements for licensure and other requirements based on geolocation can prove to be a hurdle for telehealth providers in relation to patient data collection, patient data storage and mandatory tests during the provisioning of healthcare services.
  Payments ecosystem: Since telehealth cuts across multiple geolocations, areas that have adopted online payment methods and mobile money appeal to telehealth providers.
  Inadequate regulation: The digital health space is mostly unregulated. The convergence of information technology with healthcare requires regulation that contemplates both instances, which is yet to be enacted in the Kenyan legal space.
  The recently enacted Data Protection Act, 2019 addresses data subjects' privacy and as such any data controller or processor is expected to be compliant.
- **Robotics**
  Ethical concerns regarding robotics are a key issue. Questions arise as to how the innovation was achieved, the practice of use and types of robotics used, whether collaborative or embedded.
- **Wearables**
  Its challenges cut across those of telehealth and do it yourself (DIY) healthcare practices. A key issue is unsolicited diagnosis which is only justified when, in the case of using a mobile application, it is from a regulated and licensed healthcare institution or a third party that has partnered with such an entity.
- **Virtual Assistants (e.g. Alexa)**
  The main issue regarding Virtual Assistants is how the collection and processing of data is done. These factors are mostly guided by the rights of the data subject as provided for in the Data Protection Act, 2019. Another key issue is lack of certification for healthcare diagnosis.
- **Mobile Apps**
  Key issues regarding mobile applications are ideally centred on Intellectual Property rights granted to the developers of the product. Additional concerns include: guarantee of data privacy; consumer protection issues revolving around consumer terms and conditions; limited internet connectivity and poor mobile phone market penetration rates.
- **Software as a Medical Device**
  A key issue is the user's trust of the software which hampers its acceptance in the healthcare ecosystem. Additionally, stifling regulatory requirements are a hurdle to the full implementation of software in offering healthcare solutions. Data privacy laws regard a patient's health data as a special category of data that has to be handled in a special way and this does not leave a lot of wiggle room for innovative technologies.
- **AI-as-a-Service**
  Unsolicited diagnosis is an issue that cannot be ignored, as well as collection of personally identifiable information which can easily lead to profiling that is regulated under the Data Protection Act.
- **IoT and Connected Devices**
  The challenges associated with the application of these include: human device interaction; interoperability of various IoT devices; and data sharing with healthcare providers and other third parties. There are a lot of grey areas that need to be addressed by the law.
- **Natural Language Processing**
  Issues unique to this include but are not limited to: bias on accents; lack of adequate regulation; and lack of certification for healthcare diagnosis.

3.2 What are the key issues for digital platform providers?

Data Protection: Digital platform providers who process personal information are required to be compliant with Article 31 of the Constitution which guarantees privacy for all citizens in relation to their personal information. The DPA (2019) also provides in detail requirements to be satisfied by all data controllers and processors before processing any personal information relating to Kenyan residents.

Cyber security: The Data Protection Act imposes some cyber security requirements on data controllers and processors of personal information. Notably, Kenya has domesticated the Budapest Convention on Cybercrime in the form of the Computer Misuse and Cybercrimes Act.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The use of personal data is primarily governed under the provisions of the DPA which heavily mirrors the GDPR (The General Data Protection Regulation 2016/679).

When processing personal data, data controllers and processors ought to ensure that: personal data is processed in accordance with the data subject's right to privacy; it is processed in a lawful and transparent manner; collected for an explicit purpose that is specific and legitimate; adequate, relevant and limited to

© Published and reproduced with kind permission by Global Legal Group Ltd, London

the necessary data; accurate and up-to-date with the availability of correction without delay; stored for no longer than required for the intended purposes; and is portable outside Kenya, but only upon consent and proof of adequate safeguards.

4.2 How do such considerations change depending on the nature of the entities involved?

The prevailing right that accrues in processing a data subject's personal information is consent. Data controllers and processors have a duty to notify and inform the data subject on aspects regarding the processing of personal data. However, exceptions to consent exists for the purposes of: legal compliance; public interest; or statutory tasks.

In addition, exercise of rights of data subjects may vary depending on the circumstance of the subject, i.e. where the data subject is a minor and where the data subject has a mental incapacity. In both instances, consent has to be sought from the parent/guardian/administrator.

4.3 Which key regulatory requirements apply?

The use of personal data is primarily governed under the provisions of the Data Protection Act. The DPA gives effect to Article 31 (c) and (d) of the Constitution of Kenya that guarantees the privacy of every person, including the guarantee that they do not have information relating to their family or private affairs unnecessarily required or revealed and not to have the privacy of their communications infringed on.

4.4 Do the regulations define the scope of data use?

Amongst the principles set out in the Act is that the data processor and controller must limit the use of the data to the specific purpose for collecting such information.

A data subject has rights which includes the right to be informed of the use to which their personal data is being put.

4.5 What are the key contractual considerations?

Contracts relating to the collection and processing of data ought to be compliant with the DPA to avoid non-compliance and subsequent penalties. Organisations must consider whether they fall under the category of controller or processor to cater for the responsibilities and relevant liability terms in their contracts. Controllers ought to ensure that their processors sign data processing agreements and that they guarantee certain technical measures are in place in accordance with the DPA. Data residency and data base rights are key terms that should be included in the contracts. Intellectual property rights should also be addressed. Parties that integrate with others should satisfactorily address the issue of exit in case of a termination of the relationship so that the transition is not disruptive to the business and data subject rights are not breached in any way. The data subject onboarding process has to factor in the principles of the Data Protection Act which includes transparency, adequate information and scope of processing the data, as well as the express consent of the customer.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Some key issues to consider are: the rights of a data subject; the category of the data in question, e.g. special categories; obligations relating to transfer of data out of Kenya; express consent of the data subject; consumer protection issues; and any prescribed data sharing code by the relevant authority.

5.2 How do such considerations change depending on the nature of the entities involved?

In certain circumstances, data controllers or processors are required by law to share certain personal data with e.g., regulators or authorities.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Parts VI and VII of the Data Protection Act will apply when regulating the sharing of data. These relate to the transfer of personal data and exemptions extended to the transfer.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patents in Kenya provide government-granted exclusionary rights for an "invention". Kenya has specific legislation governing patent protection in the form of The Kenya Industrial Property Act of 2001 (**KIPI**). A registered patent is protected for a period of 20 years.

It takes approximately four years to complete the process of registration. The Act expressly prohibits patenting of plant varieties as provided for in the Seeds and Plant Varieties and inventions contrary to public order, morality, public health and safety, principles of humanity and environmental conservation.

6.2 What is the scope of copyright protection?

Copyright protection in Kenya extends to work that is of an original character and has been reduced in material form. Literary, musical, artistic and audio-visual works, sound recordings and broadcasts are all eligible for copyright protection. The Copyright Amendment Act of 2019 amended the Copyright Act of 2001 (**Act**) widened the range of protected subject matter under the Act. The protection period for copyright works is dependent on the category of type.

6.3 What is the scope of trade secret protection?

Currently, Kenya does not have a statute dedicated to trade secrets provided for under Intellectual Property-specific legislation. Enforcement of trade secrets is mostly achieved by common law and equity remedies as well as remedies available for breach of contract.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

However, Kenya is a signatory to the Agreement on Trade-Related Aspects of Intellectual Property Rights (**TRIPS Agreement**). The TRIPS Agreement contains, among others, provisions on the protection of trade secrets against their unlawful acquisition, use or disclosure by third parties.

6.4 What are the typical results on academic technology transfer rules?

Technology transfer rules in Kenya are guided by The Science, Technology and Innovation Act of 2013 and corresponding rules to the Act. The Act has made it mandatory for universities and research institutions to have IP policies and technology transfer rules. In order to harmonise the various conflicting interests of stakeholders and achieve broad-based objectives, an intellectual property management policy for universities and research and design institutions should address certain issues listed in the Act.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Protection of Software is generally covered by Copyright, Trademark and to some extent, Patents. Copyright protects the various components of a software such as source code, object code and text. Protection, however, does not extend to the underlying idea embodied in the copyrighted software, or to the medium or device used to express the software. Under Kenyan law, registration is not a prerequisite for copyright protection as protection accrues once work that is subject to copyright is reduced to material and permanent form. However, registration is still recommended as it constitutes *prima facie* evidence of copyright ownership. Copyright law currently provides the most convenient available means of encouraging software development because protection is easily obtained and at a minimal cost.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The Ministry of Health launched the Kenya Health Data Collaborative in May 2016, a mid-term review of the Kenya Health Sector Strategic Plan, a series of data analytics capacity building workshops, and workshops across 33 counties to strengthen civil registration and vital statistics (**CRVS**) have all been successfully completed with the support of HDC partners.

Parties should always be aware of issues relating to data privacy, consumer protection, intellectual property, confidentiality, etc., throughout the contracting process especially where it involves integrating systems to facilitate data flows between the parties.

7.2 What considerations apply in agreements between health care and non-health care companies?

Parties must be careful that they define the scope of their services as narrowly as possible to ensure they do not carry an inordinate amount of legal risk while ensuring compliance. Obligations of each party should be clearly outlined in the contract. Terms relating to audit rights, database rights, IT rights, termination, service level agreements, commercials, etc., must be clearly outlined.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning plays a pivotal role in research into genetics, diseases and medicine. With the advanced speed of machine learning research can be fast tracked and optimised for better results.

Machine learning has also improved the process of diagnosis. It can play a key role in the early detection of key symptoms as well as an overall improvement in the speed, quality and accuracy of diagnosis.

8.2 How is training data licensed?

Research data is often released and with this, such data (training and/or research) is required to be licensed prior to the release. There are various forms of licensing in this case. However, they all share some key elements such as an arbitration requirement, a copyleft requirement and/or intent of non-commercial (unless required to be commercial, then the licensor must be paid) parties involved and the domain of the data used (public or private data) will determine how a licence is drawn up as well as the desire to commercialise at a point or not to commercialise.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

The rights can be owned by either party involved in the development and use or a combination of the various stakeholders. An agreement should clarify who owns the particular rights. For instance, the provider of the algorithm can own a portion of the IP and another portion can be owned by the party that provides the knowledge base used to teach the AI, such as a medical institute. The ownership structure could be risk-oriented (sharing the risks involved in any wrong done by the software) or commercially-oriented.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Considerations are geared towards finding the cost of collecting, storing and operating on the data. Publicly accessible data cannot be commercialised. Data with personally identifiable information (**PII**) must be anonymised to protect the identity of the data subjects. Data that is considered to be a knowledge base built over time by the party granting access to the data may be commercialised, provided they own all rights to the data.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

The realm of digital health is vast, and it transcends everything from a simple Fitbit, m-Health, digital access to medical practitioners and storage of medical records. Accordingly, adverse outcomes also transcend from unpermitted disclosure of a data subject's medical information, to giving treatment in reliance to

© Published and reproduced with kind permission by Global Legal Group Ltd, London

inaccurate/erroneous medical data. It is crucial to note that the jurisprudence emanating from the courts with respect to digital health is still growing as the concept of digital health is also still growing, although at an exponential speed having been incorporated into the country's long-term strategic health plans.

As a general rule, the theory that applies to digital health offences is that of negligence. In Kenya, protection of health rights and digital health for that matter take a multi-statutory approach. Take a case of unpermitted disclosure, for example. Under Section 11 of the Health Act, read together with Sections 32 and 46 of the Data Protection Act as well as the medical Practitioners and Dentists Act, medical information is generally confidential unless the data subject consents to the release or in the event of other considerations such as public interest or there being a court order. Article 31(c) of the Constitution speaks to privacy and provides that personal information should not be unnecessarily revealed. Whilst the privacy of medical records enjoys this legal protection, the right to privacy is not an absolute right and it may be limited when necessary. The obligation is, however, on the data controller or processor, as the custodian of such data, to ensure that this data remains private. Under Section 32 of the Data Protection Act, where there is consent, the burden is on the data process to demonstrate so. The data controller/processor has a duty to protect the data subjects' data and where there is a breach, the courts must assess the circumstances under which such data was released and hence, breach of that duty of care.

The Court for instance in *David Lawrence Kigera Gichuki v Aga Khan University Hospital [2014] eKLR* found justification in the release of medical records and held:

i. that a medical practitioner or medical facility is under an obligation not to release confidential information about a patient without the patient's knowledge or consent;
ii. that there are, however, circumstances in which the medical practitioner or institution may be required to release such information for valid governmental and public interest reasons; and
iii. that a medical practitioner or institution may be required by law or a court order to release information about a patient without the patient's consent.

On the flipside, the Court in *Kenya Plantation and Agricultural Workers Union v James Finlay (K) Limited [2013] eKLR* found fault in the release of medical information:

"This issue is of particular concern to the court because under Sub-Article 31(c) of the Constitution, every person has the right to privacy which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed. In the opinion of the court, such right includes the right to have information such as official records, photographs, correspondence, diaries and **medical records** kept private and confidential. It is the further opinion of the court that in the instant case, the respondent in discharge of the duty to uphold medical professional ethics of its medical staff as prescribed in the Rules is obligated to take positive steps to prevent intrusions into the privacy of its hospital's patients."

Similarly, in cases where treatment has been administered based on erroneous records, there will have been a duty of care and the Court will assess, on a case-by-case basis whether there was a breach on such duty. Accordingly, any inimical consequence is tested on a case-by-case basis to establish whether there was negligence as absolute/strict liability is not applicable.

9.2 What cross-border considerations are there?

The Data Protection Act envisions situations where personal data may be transferred outside Kenya and prohibits it. Section 25(h) of the Data Protection Act prohibits the transfer of personal data with a proviso to where there has been consent or proof of data protection safeguards.

The cross-border transfer of data has room for improvement. The DPA, new as it is, also leaves room for such improvement under Section 74, which states that the data commissioner may develop sector-specific guidelines for areas such as health. This will cover situations such as hospitals that buy storage from service providers who are not in Kenya in as much as the custodian of the data is the medical facility in Kenya.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Data Sovereignty: The location of the data centre should be considered since some sectors such as healthcare information are considered to process sensitive special categories of personal data (in line with the DPA) and thus, the cloud provider should be able to impose rights relating to the data regardless of where it is hosted.

Cyber-threats: The cloud provider has the obligation to provide adequate safeguards that guard against cyber threats in accordance with the Kenya Information Act and the Computer Misuse and Cybercrimes Act.

Cloud infrastructure type: Cloud providers can consider several options such as: infrastructure as a service (**IAAS**); platform as a service (**PAAS**); and software as a service (**SAAS**). Each of these options has its own responsibilities to the cloud provider and digital healthcare provider.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Some of the key issues that non-healthcare companies should consider are:

- Applicable laws and regulation to assess the compliance requirements.
- Government Policy.
- Any applicable market standards.
- Consumer protection issues to mitigate reputation risk.
- Peculiarity of the market to assess if its facilitative or prohibitive.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

- Licensing models: Firms can exploit available intellectual property-based commercialisation tools such as licensing and franchising.
- Competition regulation: The Competition Act, 2010 is the law that regulates competition in Kenya. It prohibits restrictive trade practice, controlling mergers and acquisitions and concentration of economic power, aims to protect consumers and the public at large from unfair and misleading market.
- Taxation: The Income Tax Act and subsidiary rules guide taxation of different industries.
- Existing laws and regulations that govern such transactions.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

John M. Ohaga is the Managing Partner at TripleOKLaw LLP Advocates and is celebrated as a formidable leader in the firm and the public space as a legal practitioner. His career spans more than 26 years during which he has been involved in numerous complex litigation matters as well as high-value domestic and international arbitration cases. John is acknowledged as an expert practitioner in several areas of law such as administrative law, banking and finance, constitutional law, employment and labour law, public procurement and sports law. He advises numerous blue-chip companies listed on the Nairobi Stock Exchange, many private companies, and some of Kenya's largest state corporations. He sits on the boards of several companies and public tribunals including as Chairman of the Kenyan Sports Disputes Tribunal and the Appeals Committee of the Advertising Standards Board.

TripleOKLaw LLP Advocates
ACK Garden House, 1st Ngong' Avenue
Nairobi
Kenya

Tel: +254 709 830 100
Email: johaga@tripleoklaw.com
URL: www.tripleoklaw.com

Stephen Mallowah is a partner in the Commercial and Corporate Law Department and heads a couple of specialised practice areas in the firm. He has demonstrated expertise in several specialised areas of law, including capital markets and financial services, structured and project finance, energy, mining, oil and gas. He further provides advice to clients on regulatory compliance, public policy and legislative engagement. Steve is constantly pushing the knowledge boundary in emerging areas of practice. This is evidenced by the fact that he is one of the pioneering lawyers in Kenya in the area of Public Private Partnerships and has advised both the public and private side on large PPP projects that successfully achieved commercial and financial close. Steve also heads the firm's new Climate Change and Sustainability Practice.

TripleOKLaw LLP Advocates
ACK Garden House, 1st Ngong' Avenue
Nairobi
Kenya

Tel: +254 709 830 100
Email: smallowah@tripleoklaw.com
URL: www.tripleoklaw.com

Catherine Kariuki is a Deputy Managing partner heading the Technology, Media and Telecommunications (**TMT**) Practice and is a strong advocate for innovation in the legal space. Her work provides advisory on general commercial work, fintech-related transactions, data protection, cyber security-support in digital forensics work, privacy, ownership and governance, consumer protection, intellectual property and mobile payments. Catherine's strength in transactional work and regulatory compliance has enabled her to work seamlessly with several domestic and multi-national companies towards regulatory compliance and business processes and strategy support. Catherine is internationally recognised as a recommended lawyer for Commercial, Corporate and Mergers and Acquisitions and is a frequent speaker at digital disruption and fintech conferences and symposiums.

TripleOKLaw LLP Advocates
ACK Garden House, 1st Ngong' Avenue
Nairobi
Kenya

Tel: +254 709 830 100
Email: ckariuki@tripleoklaw.com
URL: www.tripleoklaw.com

Janet Othero is a partner and one of the brains behind our cutting-edge practice in telecommunications regulations and technology in the financial sector. She has experience in contract negotiations, regulatory due diligence and general legal advisory, having worked with several leading financial institutions. With her understanding of digital disruption, Janet continuously advises clients on the legal implications arising from cyber security to cyber resilience and handling the interrelated impact. She has also gained expertise in Fintech, Regtech, payment systems and data privacy governance. She is internationally recognised as a next generation lawyer for her work in Banking, Finance and Capital Markets and is a regularly featured speaker at conferences and symposiums on digital disruption and Fintech symposiums.

TripleOKLaw LLP Advocates
ACK Garden House, 1st Ngong' Avenue
Nairobi
Kenya

Tel: +254 709 830 100
Email: jothero@tripleoklaw.com
URL: www.tripleoklaw.com

TripleOKLaw LLP is a full-service law firm founded in Kenya in 2002. The firm is renowned for its innovative and professional legal services in the local and international space.

A strong background in corporate and commercial law practice coupled with robust technology-based internal systems inspired a well-informed and practised Telecommunications, Media and Technology team. The innovative practice area advises clients on regulatory compliance, data protection and policies, digital forensics and more aspects affecting clients in the telecommunications, fin-tech, payments and technology industries.

The firms commercial work supports our clients' various needs in legal advisory services on mergers & acquisitions, legal due diligence, joint ventures, corporate restructurings, public private partnerships, corporate governance, regulatory compliance, company secretarial services and commercial contracting.

www.tripleoklaw.com

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Korea


Won H. Cho


Shihang Lee

D'Light Law Group

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

"Digital Health" (sometimes interchangeable with "Smart Health") is not a legally defined term but has been widely used by the government or in the market as an umbrella term to categorise the industry area in which IT and healthcare are combined.

1.2 What are the key emerging technologies in this area?

Medical Big Data Analysis/AI, Wearables, SAMS (and DTx), AR/VR, etc.

1.3 What are the core legal issues in health care IT?

From the contractual side, (1) patent registration and (2) licensing of target technology can be named as core issues. From the regulatory side, (1) processing of personal and/or medical information, (2) obtaining marketing approvals for medical device (including the proof of safety and efficacy), and (3) getting pricing approval to be covered by the National Health Insurance system.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The respective authorities regulate (1) funding for research & development, (2) manufacture and marketing of medical devices/products, (3) medical services performed and medical records produced by doctors and medical institutions, and (4) reimbursement of medical insurance.

2.2 What other regulatory schemes apply to digital health and health care IT?

The collection, processing and other use of personal information is regulated under the "Personal Information Protection Act" and that of medical records is under the "Medical Services Act". The "Bioethics and Safety Act" may apply in certain cases.

2.3 What regulatory schemes apply to consumer devices in particular?

Consumer devices in principle are not supposed to provide "medical services" which are mandated to be performed by doctors. If classified as non-medical services, more general regulation on the safety of electronic devices may be applied.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The MSIT (Ministry of Science and ICT) and the MOTIE (Ministry of Trade, Industry and Energy) are the main authorities that govern the R&D funding.

The MFDS (Ministry of Food and Drug Safety; a rough equivalent of the FDA) governs: the manufacturers and distributors; pre-clinical and clinical trials; marketing authorisation; safety control (post-marketing surveillance); and other safety-related administrative measures.

The MoWH (Ministry of Health and Welfare) governs the doctors and medical institutions (e.g. clinics, hospitals), medical services and (electronic) medical records.

The NHIS (National Health Insurance Service) and the HIRA (Health Insurance Review and Assessment) govern the National Health Insurance which is the mandatory, government-driven, largest medical insurance that covers almost all Korean citizens; secondhandedly, they govern the manufacturers and distributors, doctors and medical institutions, as well as patients through pricing approvals and reimbursement.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

Safety and efficacy, fiscal viability, legitimate processing of personal information and/or medical information from EMR.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Software as a Medical Device (SAMD) has been categorised as part of medical devices and thus the conventional authorisation (permission, certificate or notification) process has been applied, which requires evidences of safety and efficacy. A new legislation which will be in effect from May 2020 sets forth an expedited procedure for innovative SAMD.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Telehealth is in principle prohibited under Article 34 (Remote Medical Treatment) of the Medical Services Act. This has been one of the most disputed subjects among the stakeholders. A government-led experimental project that allows Telehealth within a restricted area is currently on-going.
- **Robotics**
  Robotics is mainly applied to rehabilitative medicine and the rather conventional legal issues as addressed in section 2 apply.
- **Wearables**
  If a wearable is a medical device under the definition of the Medical Device Act, or provides services which the government deems to require the supervision of medical professionals, then a set of robust regulations as in section 2 apply. Wearables that are not medical devices may face data privacy issues if they collect and process health-related data from the users.
- **Virtual Assistants (e.g. Alexa)**
  Virtual Assistants' main role is to "help" (rather than to "replace") medical professionals in making decisions in a more cost and time efficient manner. Liability issues (i.e. who is in charge, the machine or the doctor) rarely arise as the application of such virtual assistants is not widespread yet. However, the main obstacle is that Electronic Medical Records (EMR) and other health-data are strictly regulated, so "feeding" data to the Virtual Assistants is not easy.
- **Mobile Apps**
  Mobile Apps currently seem to be divided into "Medical" Apps, which mostly function as advertisement platforms which often causes regulatory issues, and "Lifestyle" Apps, which act as coaches for exercise, diet, meditation, etc.
- **Software as a Medical Device**
  The cases in which SAMD has been approved are mostly coupled with the Hardware Medical Device that contains it within. The MFDS is aware of, as described in its guideline revised in September 2019, the possibility of independent SAMD and other more recent types of SAMDs.
- **AI-as-a-Service**
  If we can roughly define AIAAS as "implementing AI in the Cloud Server and providing it to customers", such concept is quite new especially in the Korean healthcare industry.
- **IoT and Connected Devices**
  This field is on an emerging level and data security can be named as a possible issue.
- **Natural Language Processing**
  The application of NLP technology in this industry is still limited.

3.2 What are the key issues for digital platform providers?

Medical Data Platforms face restrictions in acquiring and processing high-quality yet sensitive medical data (e.g. EMRs). Other types of platforms such as information, advertisement and/or community platforms are more concerned about complying with conventional regulations (e.g. the Medical Services Act).

4 Data Use

4.1 What are the key issues to consider for use of personal data?

PIPA (Personal Information Protection Act) is the main governing law on the use of personal data. The consent of the data subject should be acquired to collect, process, share, etc. the personal information. In the case of "sensitive information" which includes information on the data subject's health, stricter regulation applied as a separate procedure to obtain such data subject's consent is required. Access to "medical records" is very limited and allowed in exceptional cases such as being required in civil or criminal procedure, according to the Medical Services Act. In January 2020, however, the regulation over personal data has been mitigated to allow broader use of pseudonymised personal data.

In terms of human genetic data, the Bioethics and Safety Act applies, which is in part stricter than PIPA. However, similar legislation was made in January 2020 to expand the category of authorised DTC (Direct-To-Customer) genetic sequencing services; services which are predominantly provided by only four companies.

4.2 How do such considerations change depending on the nature of the entities involved?

"Personal information controller", which is the entity that processes personal information to operate the personal information files for official or business purposes, bears various obligations under PIPA. In case of public institutions backed up by law to process personal information, such obligations are alleviated. Otherwise, the nature of the information affects more than the nature of the entities that process such information.

4.3 Which key regulatory requirements apply?

PIPA requires that: (1) the purpose of the collection and use of personal information are disclosed; (2) particulars of personal information to be collected are disclosed; (3) the period for retaining and using personal information is disclosed; (4) the fact that the data subject is entitled to deny consent, and disadvantage affected resultantly from the denial of consent; and (5) the third party recipient of personal information and its respective details from (1) through (4), is disclosed, if applicable. Personal information controllers focus on informing and getting consent from data subjects with respect to the items (1) through (5) above.

4.4 Do the regulations define the scope of data use?

The scope of data use is not defined by legislations but rather construed by agreements between data subjects and personal data controllers.

4.5 What are the key contractual considerations?

Data subjects in many cases provide their consent in consideration of the services that personal information processors provide (e.g. signing up on a website). Direct "sales" of personal information from an individual to an entity is rare and its legitimacy under the legal system in the territory is in question, meanwhile, the DTC genetic sequencing market has been growing gradually.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

However, the government has been funding the NGS (New Generation Sequencing) for cancer patients *via* National Healthcare Insurance coverages and thus indirectly collecting such genetic data from a considerably large cohort. Some professionals from the clinical and academic fields have increased applied and/or commercial use of such NGS data for the benefit of the public.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The consent of the data subject for sharing personal information is required. Anonymised personal data is precisely not "personal information" following its definition in PIPA and can be shared without infringing the Act. Sharing pseudonymised personal data is levied with far fewer obligations (such as mandatory obtainment of consent from the data subject prior to the sharing of personal data), than normal personal data, and legislative discussion as of January 2020 has been going advantageously for semi-free sharing.

5.2 How do such considerations change depending on the nature of the entities involved?

As previously mentioned in question 4.2, the nature of the information is more critical than the nature of entities involved unless such entities are public institutions that enjoy legal privileges.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Consent from the data subject is required. For details, please see question 4.3.

6 Intellectual Property

6.1 What is the scope of patent protection?

According to the Patent Act, an invention can be granted a patent if it (1) is a highly advanced creation of a technical idea utilising the laws of nature, (2) has industrial applicability, and (3) is not publicly known prior to the filing of a patent application. Korea is a member of WIPO PCT (Patent Cooperation Treaty). It would be worth noticing that Approval-Patent Linkage System, a rough equivalent of the Hatch-Waxman Act in the U.S., has been in effect since 2015.

6.2 What is the scope of copyright protection?

According to the Copyright Act, "work" to which copyright is entitled is a "creative production that expresses human thoughts and emotions". The author's moral and economic rights are protected in different ways. Korea is a member of TRIPs, the Berne Convention, WCT and other treaties pursuant to copyright protection.

6.3 What is the scope of trade secret protection?

According to the Unfair Competition and Trade Secret Protection Act, the term "trade secret" means information, including a production method, sale method, useful technical or business information for business activities, that is not known publicly, is the subject of reasonable efforts to maintain its secrecy, and has independent economic value. In practice, non-disclosure clauses or agreements can set forth a narrower or broader scope of trade secrets by adding or alleviating requirements.

6.4 What are the typical results on academic technology transfer rules?

Most academic inventions (in many cases, employee inventions) initially get to belong to the institution following the contracts between the inventor and the institution, or the guidelines, rules and/or laws that govern them both. The institution or its representative (e.g. University-Industry Foundation) may transfer or license-out the technology to corporates or other entities in consideration of payments of which styles can vary (e.g. upfront, milestone, royalty, etc.). Both the "technology market" and the government have great interest in "technology commercialisation" and there exists a portfolio of laws attempting to promote technology commercialisation.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Neither SAMD nor computer software is explicitly categorised within the scope of patent protection, but computer software has been protected as the subject of patent by judicial precedents and KIPO (Korean Intellectual Property Office)'s guidelines. The source code of software has been protected by copyright laws as well. Since the Patent Act describes "utilising the laws of nature" as one of the requirements to be a patentable invention, SAMD shall entail some hardware portion which executes itself in order to have patent protection.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Treatment to collaborative improvements may vary by each agreement that governs them. The licensor may block any emergence of improvements by explicitly prohibiting the licensee from making any attempt to produce improvements, or claim for the ownership of any improvement, or plan ahead a good faith negotiation over such ownership. Even in the cases where the licensee pays considerable reward for using the original invention, the licensor often insists on the sharing of data or other outcomes produced by the licensee.

7.2 What considerations apply in agreements between health care and non-health care companies?

Collaborations do happen between "healthcare companies" and "non-healthcare companies", but such non-healthcare companies nonetheless have certain understanding of the industry prior to such collaborations, and therefore the agreements between them do not seem to have "peculiar" considerations as compared to agreements amongst healthcare companies. Non-healthcare companies are mostly investors and in their investment agreements they demand healthcare companies of certain representations and warranties over the technological aspects.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Currently machine learning is most widely used in diagnostics, especially in analysis of medical images such as CT, MRI, PET, angiography, etc.

8.2 How is training data licensed?

Neither legal disputes over, nor commercial trading of, training datasets has become significant in the territory. In the health-care industry, developers from companies often gain access to datasets by performing collaborative research or clinical trials with doctors from medical institutions. In many cases, such research or clinical trials are funded by the government and are therefore financially beneficial for both parties.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

The copyright on AI-created algorithms are still under debate albeit such concept is yet to be accepted generally. KIPO and other government institutions have conducted some research on the possibility of such right, or at least, such concept.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Currently, most training datasets are acquired directly from data subjects, for which personal data privacy is the main issue. Terms of use and privacy policy are two main agreements contracted between the data subject and the data processor. The data processor must comply with PIPA and other relevant rules. (Please see section 4 and 5 for more details.) In case a data processor shares data with a third party, such third party may need to ensure that the data-providing party fully complies with regulations, and representation & warranty clauses may be useful for such purpose.

A few cases of commercial trading of datasets exist, but even in such cases, milestone payments or royalties for the future are often preferred to upfront payments.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Contractual default and tort are two main theories. Relatively stricter liability may apply to manufactured goods and to medical malpractice. Aside from civil liability, administrative measures such as recall and prohibition of sales may be imposed on the manufacturer and/or seller, depending on the cause of damages.

9.2 What cross-border considerations are there?

In transnational businesses, the parties may consider which party shall hold the marketing authorisation and/or price approvals as such party will directly bear the obligations and be subject to regulatory dispositions.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based service providers must follow the obligations pursuant to data privacy as set forth in PIPA and other rules. (Please see sections 4 and 5 for more detail.) One of the hottest issues in cloud-based services is that EMR must be stored in servers physically located within the territory, which has caused much controversy among the entrepreneurs attempting cloud-based processing of medical records.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Non-healthcare companies are highly recommended to make efforts in understanding the regulatory schemes before entering the digital healthcare market. Even the multinational electronics corporations based in Korea have been reluctant to expand their business portfolio to the digital healthcare market, mostly because of regulatory issues.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

Technological or regulatory viability of the transferred or licensed technology, product and/or compound should be examined with scrutiny before making investment decisions. It is recommended to evaluate digital healthcare ventures with caution as their value is often exaggerated in the market, especially for unlisted companies. There is also the risk of policy change as the healthcare industry has been officially announced as one of three "national future industries" and lots of discussions are ongoing in both policymaking and legislative sectors.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Won H. Cho is a managing partner at D'LIGHT. As an experienced patent lawyer with extensive commercial transactional experience in various specialty industries including entertainment, ICT and healthcare, Won H. Cho is uniquely positioned to advise clients on a wide range of complex IP, corporate and regulatory matters. He started his career as an associate at Bae, Kim & Lee LLC ("BKL") and went on to serve as a partner of the firm, leading BKL's prominent intellectual property and technology transaction practices, spanning a total of 16 years. Mr. Cho also worked on secondment at Ropes & Gray (New York) in 2014 in the firm's Intellectual Property division. He has earned a reputation at home and abroad as an exceptional multi-disciplinary lawyer with deep and extensive career experience, representing local corporations, multi-national companies, government agencies and non-profit organisations. Mr. Cho is now an adjunct professor at KAIST-MIP (Master of Intellectual Property) and serves in leadership roles at various local and state organisations, including the Korea Fair Trade Commission Advisory Committee, Korean Intellectual Property Office, US Korea Law Foundation, Korea Licensing Executive Society, and the Korea Association of Entertainment Law, among others. Mr. Cho holds a B.A. from Seoul National University and received an LL.M. from the University of Texas.

D'Light Law Group
5th floor, 311, Gangnam-daero
Seocho-gu
Seoul 06628
Korea

Tel: +82 2 2051 1870
Email: whc@dlightlaw.com
URL: http://eng.dlightlaw.com

Shihang Lee works in D'LIGHT's Healthcare group, focusing on all aspects of the healthcare industry including IP, Regulation, Licensing & Corporate issues. Mr. Lee studied Bioengineering under the rigorous discipline of UC Berkeley College of Engineering, which included concentration gradient modelling of pharmaceutical patches, and construction of EKG devices from scratch, etc. Mr. Lee served as a public-service advocate in the Ministry of Food and Drug Safety in Korea.

D'Light Law Group
5th floor, 311, Gangnam-daero
Seocho-gu
Seoul 06628
Korea

Tel: +82 2 2051 1870
Email: shl@dlightlaw.com
URL: http://eng.dlightlaw.com

D'LIGHT is a premier specialty law firm offering more than just legal services – we offer a unique specialisation perspective for commercial thinking and legal problem-solving.

In today's fast-changing and volatile market conditions, effective legal service demands much more than skilled advocacy. Whether a business is looking to start up, establish a strategy for growth or plan for exit, D'LIGHT provides real practical solutions and applied expertise that help turn ideas and ambition into success.

At D'LIGHT, our unrivalled specialty knowledge and deep industry experience allow us to creatively improvise on and innovatively resolve even the most difficult commercial issues. Our experience is a testament to our deep understanding, appreciation and proven capability to problem-solve (not simply "issue-spot") on challenging and novel legal matters that are driving increasingly complex transactions today.

In our approach to work, we do not consider the practice of law a job, but rather a calling to serve our clients, the profession and the community. We take a genuine partnership approach in working with our clients, focusing not just on what they want, but on how they want it. Always pushing the boundaries of what can be achieved, we strive to reshape the legal market and challenge our clients to think differently about what a law firm can be.

www.dlightlaw.com

D'LIGHT
D'LIGHT Law Group

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Mexico


Abraham Díaz


Ingrid Ortíz

OLIVARES Y COMPAÑIA

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

Mexican legislation has not specifically defined "digital health". However, the Federal Commission for the Protection against Sanitary Risks (COFEPRIS) and other private and public entities are already addressing the matter in various aspects (i.e. regulation, guidelines, analysis, forums, and others).

1.2 What are the key emerging technologies in this area?

Many areas of health technology are rapidly developing in Mexico, such as: mobile apps; robots; 3D printing; telemedicine; machine learning; genome research; and drones and healthcare.

In relation to the above, most recent advances in digital health in Mexico have been mainly applied to three diseases: ischaemic heart disease, breast cancer and diabetes. For example, with advances in the genetic analysis of diabetes, Mexican doctors and scientists may be able to predict which students within a student population are likely to develop diabetes, and therefore intercept with preventative measures that will save many costs in the future.

1.3 What are the core legal issues in health care IT?

As a type of medical device aimed to be used by healthcare practitioners and patients, healthcare IT has safety, quality and effectiveness implications. This is currently regulated by COFEPRIS, which grants marketing authorisations to products that are safe and effective.

Data protection is another important issue in the field of healthcare IT. IT often involves the collection and/or transfer of data, and healthcare IT could involve the collection and transfer of sensitive data. The mechanisms of data protection in Mexico are discussed further below.

It is advisable that entities offering healthcare IT are aware of professional liability issues, and that they check whether their professional liability insurance covers things that go wrong when providing healthcare IT services, including providing services that require a medical licence or administering medical care.

2 Regulatory

2.1 What are the core health care regulatory schemes?

Although developing, the field of digital health is still relatively new in Mexico and its application in real-life settings is still limited. There are no specific healthcare regulatory schemes for digital health; the field is instead being covered by schemes which regulate medicinal products and medical devices, namely:

- the General Health Law (in Spanish, "*Ley General de Salud*");
- the Health Law Regulations over Healthcare Products (in Spanish, "*Reglamento de Insumos para la Salud*");
- Official Mexican Standards (NOMs), particularly the NOM-241-SSA1-2012 setting good manufacturing practices for medical devices and NOM-137-SSA1-2008 for the Labelling of Medical Devices;
- the Mexican Pharmacopoeia;
- COFEPRIS' Rules listing healthcare products that do not require a marketing authorisation due to low risks on human health (published in December 2014).

COFEPRIS may already be addressing the need for regulations for mobile medical applications, especially for those that present health risks.

2.2 What other regulatory schemes apply to digital health and health care IT?

Since digital health and healthcare IT implies health information management across computerised systems and the secure exchange of information between consumers, providers, payers and others, it is necessary to keep in mind the compliance with data protection laws in Mexico, as well as regulations dealing with e-commerce and electronic payments.

2.3 What regulatory schemes apply to consumer devices in particular?

Consumer devices require marketing authorisations from COFEPRIS in order to be marketed in Mexico. Marketing authorisation requirements, for medical devices in particular, depend on the level of risk involved in their use, according to a threefold classification system:

- Class I: products that are well-known in medical practice and for which safety and efficacy have been proven. They are not usually introduced into a patient's body.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- Class II: products that are well-known in medical practice but may have material or strength modifications. If introduced, they remain in a patient's body for less than 30 days.
- Class III: products either recently accepted in medical practice or that remain in a patient's body for more than 30 days.

The Mexican Pharmacopoeia provides manufacturers with specific rules and examples as guidance to classify medical devices.

Furthermore, COFEPRIS published a list of medical devices in 2014, which specifies which devices do not require regulatory approval in order to be marketed and sold in Mexico. Such products are usually those that are low risk to a patient's health.

In addition, since consumer devices are also collecting and transferring personal information to various parties, it is also necessary that they comply with data protection laws in Mexico, as well as with regulations dealing with e-commerce and electronic payments.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The Mexican authority responsible for enforcing the regulatory framework is COFEPRIS. COFEPRIS analyses all medical devices, and if applicable, software that enables them to work.

Additionally, the National Center of Health Technology Excellence was created in order to develop guidelines to evaluate health technologies and clinical practices and manage medical equipment and telemedicine.

The National Institute of Transparency, Access to Information and Personal Data Protection (INAI) is the authority responsible for overseeing the Law. Its main purpose is the disclosure of governmental activities, budgets and overall public information, as well as the protection of personal data and the individuals' right to privacy. The INAI has the authority to conduct investigations, review and sanction data protection controllers, and authorise, oversee and revoke certifying entities.

The Ministry of Economy is responsible for informing and educating about the obligations for the protection of personal data between national and international corporations with commercial activities in the Mexican territory. Among other responsibilities, it must issue the relevant guidelines for the content and scope of the Privacy Notice in cooperation with the INAI.

The Federal Consumer Office (PROFECO) monitors the compliance of the applicable provisions concerning information and advertising which could also be applicable to digital health. Additionally, PROFECO observes that "information or advertising of goods, products or services that are disseminated by any means or form must be truthful, verifiable, clear and free of texts, dialogues, sounds, images, trademarks, appellations of origin and other descriptions that lead or may lead to misleading, confusing, deceptive or abusive information".

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

COFEPRIS can initiate *ex officio* legal proceedings to sanction non-compliance. Ultimately, these legal proceedings can result in the revocation of the marketing authorisation. COFEPRIS is also entitled to implement measures on behalf of public health, such as the seizure of products and ordering partial or total suspension of activities, services or adverts. Under certain conditions, COFEPRIS has statutory authority to revoke any manufacturing approval or impose sanctions, ranging from a fine of up to 16,000 times the minimum wage to closure of the establishment.

The imposition of administrative sanctions does not exclude civil and criminal liability. Administrative infringements can incur penalties ranging from a fine of up to 20,000 times the minimum wage to final closure of the establishment. Repeated infringement is also considered to be a criminal offence.

COFEPRIS has broad jurisdiction to seize counterfeit or illegal devices. The General Health Law classifies the manufacturing and sale of counterfeit or falsified devices as a crime. In addition, COFEPRIS commonly enters into collaborative agreements with the PGR and the Customs Office in order to investigate and prevent counterfeit and illegal devices from entering the Mexican market.

In accordance to the Federal Law on Protection of Consumers, the Federal Consumer Office can monitor the compliance of the applicable provisions concerning information and advertising which could also be applicable to digital health. This Law provides that "information or advertising of goods, products or services that are disseminated by any means or form must be truthful, verifiable, clear and free of texts, dialogues, sounds, images, trademarks, appellations of origin and other descriptions that lead or may lead to misleading, confusing, deceptive or abusive information". In addition, the provider of goods and services is obliged to comply with the specifications of the goods or services offered.

Since all information dealing with consumer's health is deemed to be sensitive, affected consumers of digital health devices or services may request INAI to initiate an investigative process in case of a data breach, or in case of any other violation to the health information of a data subject. INAI, attending said complaint or *ex officio* may initiate the investigative process and if it considers that there was any data breach or any other violation to Mexican Data Protection Laws, it may impose administrative sanctions such as fines up to MXN$25,000,000 (approximately USD$1,400,000).

Additionally, there are two activities deemed as felonies related to the wrong use of PI, which are:

i) When a data owner authorised to collect, store and use PI with the aim of profiting, causes a security breach in the database containing PI under its custody. This is sanctioned with imprisonment from three months and up to three years.

ii) To collect, use or store PI, with the aim of profiting, through error or deceit of the data subject, or error or deceit of the person who has to authorise the transfer. This is sanctioned with imprisonment from six months and up to five years.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

There are no specific regulations that apply to Software as a Medical Device and its approval for clinical use. As mentioned above, medical devices, a group under which digital technologies would currently fall, would require a marketing authorisation from COFEPRIS in order to be marketed and sold in Mexico.

So far, the regulations applicable to Software as a Medical Device are those mentioned in the answer to question 2.1. However, COFEPRIS may already be addressing the need for regulation of digital health technologies, especially for those that may present health risks.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  In Mexico, telehealth is understood to include all aspects of incorporating information and communication technology (TIC) into health systems, with the aim of exchanging information in the field of health.
  If providing medical attention or services that require a medical licence *via* telehealth, it is important to consider professional liability and whether insurance policies cover such services.
  Furthermore, if personal or sensitive personal information is collected or transferred, entities will need to be aware of the legal implications, which are discussed further below.
- **Robotics**
  Robotics, particularly robotic surgery, has advanced to a world-class standard in Mexico. However, risks still exist, and again, liability is an important consideration for when things go wrong. Legislation in Mexico is yet to be developed to cover such situations.
- **Wearables**
  As explained above, a medical device is defined as to be used in the diagnosis, monitoring or prevention of diseases in human beings, or in the treatment of those diseases or disabilities, as well as in the replacement, correction, restoration or modification of human physiological processes or anatomy.
  Whether a "wearable" or smartwatch will be considered as a medical device will depend on the specifications of such device and its purpose.
  In the List of Medical Devices that do not require regulatory approval, stopwatches are included ("*Relojes de tiempo transcurrido*"). Therefore, depending on the function of the particular wearable, regulatory approval may or may not be required.
- **Virtual Assistants (e.g. Alexa)**
  In Mexico, Virtual Assistants are used in the healthcare sector to schedule patient appointments. Virtual Assistants involve intelligent bots to organise, confirm and cancel appointments without any need for human intervention.
  Given that this technology stores information on the Cloud, an important consideration is data security and privacy. This is discussed in more detail below.
- **Mobile Apps**
  As explained for telehealth, medical mobile application developers or entities that deliver services through the same will need to be aware of any professional liabilities or licences required when providing medical services or advice.
  In relation to regulatory approval, COFEPRIS may already be addressing the need for regulations for mobile medical applications, especially for those that present health risks.
- **Software as a Medical Device**
  Due to its nature, it is common that Software as Medical Device in Mexico involves data collection, so if personal or sensitive personal information is collected or transferred, entities must be aware of the legal implications, which are discussed further below.
  In addition, it is worth considering that patent protection is not available for software as such, unless it implicates computer-readable claims which meet the patentability requirements in its methodology and functions involved. Also, copyright protection is available for software.
- **AI-as-a-Service**
  In Mexico, the most recent development of Artificial Intelligence in health is the use of AI as a Service for the analysis of cancer data. The requirement of large amounts of data for AI means the risks of data security and privacy must be considered, particularly because the data used, i.e. sensitive medical data, has higher legal requirements.
- **IoT and Connected Devices**
  Similar to the above, applying IoT and Connected Devices to the healthcare sector carries risks in data security and privacy. The close monitoring of this technology and the implementation of safeguards is crucial when using it in a medical setting.
- **Natural Language Processing**
  As mentioned above in the answer to Virtual Assistants, Natural Language Processing tools such as chatbots can be applied in the healthcare sector to program medical appointments and answer frequently asked questions without the need for human intervention.
  Given that this technology stores personal information on the Cloud, an important consideration is data security and privacy. This is discussed in more detail below.

3.2 What are the key issues for digital platform providers?

The key issues that should be taken into consideration by digital platform providers are:

- Safety.
- Quality.
- Effectiveness.
- Data protection.
- Tax (see question 7.2).

These providers should carefully monitor changes to the legislation given that this field is still developing in Mexico.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The main issues are the scope of data storage, processing and sharing, the requirement to appoint a data protection officer and how to manage data security and data breaches.

- The key issue to consider, regarding personal information in digital health, is that all information regarding the health of any data subject is deemed to be sensitive. Therefore, the basis for the collecting, processing, sharing or transferring of said information, is the consent of the data subject, being the case that when dealing with sensitive information, the consent must be expressed in writing (consent obtained through digital means is acceptable, but the data subject must express his/her consent through an active process such as an opt-in mechanism, without any pre-checked boxes).
  It is also important to remember that an exception for the obtaining of the consent of the data subject, for the collection, use and transfer of his/her personal information, is when said personal information is essential for certain medical or health matters where the individual is unable to provide consent.
- In Mexico, there is no regulation dealing with the sharing of data that does not constitute personal information. In

© Published and reproduced with kind permission by Global Legal Group Ltd, London

other words, if the information to be shared between two or more parties involved in digital health is not personal information as set forth in Mexican law, then it can be shared. This may change in the future, since international trends are starting to impose some restrictions on data sharing, which may be adopted in the future by Mexico.

4.2 How do such considerations change depending on the nature of the entities involved?

Although in Mexico we have two different bodies of law regulating the protection of personal information, depending on whether the data collector or data processor belongs to the public administration, or whether it is a private entity; the principles for the collection, use, sharing and transfer of data are basically the same, the key principle and basis for the treatment being the consent of the data subject.

4.3 Which key regulatory requirements apply?

The principal data protection regulation is found (i) in Articles 6 and 16 of the Mexican Constitution, and (ii) in the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations, published in July 2010 and December 2011 respectively.

Other applicable regulations include:

- The General Law for the Protection of Personal Data in the Possession of Obliged Subjects, which regulates the processing of personal information in any Federal, State or local authority's possession.
- The Privacy Notice Rules.
- The Binding Self-Regulation Parameters.

In general, Mexican data protection laws follow international correlative laws, directives and statutes, and therefore have similar principles, scopes of regulation and provisions.

The key principles that apply to the processing of personal data are:

- Transparency – although not specifically defined, the Law clearly states that personal data cannot be collected, stored or used through deceitful or fraudulent means.
- Lawful basis for processing – the collector is responsible for processing personal and/or sensitive data in accordance with the principles set forth in the Law and international treaties.
- Purpose limitation – personal data shall only be processed in compliance with the purpose set out in the Privacy Notice.
- Data minimisation – the collector shall make reasonable efforts to ensure that the amount of personal data processed is as little as necessary according to the purpose.
- Proportionality – data controllers can only collect personal data that is necessary, appropriate and relevant for the purpose.
- Retention – the collector can only retain personal data for the period of time necessary to comply with the purpose, and is obliged to block, cancel or supress the personal data thereafter.

4.4 Do the regulations define the scope of data use?

The regulations define "processing" as the collection, use, disclosure or storage of personal data, by any means. The use covers any action of access, management, benefit, transfer or disposal of personal data.

"Personal data" is defined as any information concerning an individual that may be identified or identifiable.

4.5 What are the key contractual considerations?

From the data protection standpoint, the main key contractual consideration to be observed is that the data collector is responsible for any processing of personal information carried out by the data processors that it decides to use for the operation of digital health devices or services. Therefore, in accordance with Mexican law, the data collector must make sure that the data processors that it employs assumes the same obligations as the data collector, towards the personal information of the data subjects. For this purpose, it is convenient to use binding corporate rules or standard contractual clauses.

If a processor is appointed to process personal data on behalf of a business, there must be a contract in place to establish the scope of the relationship.

The agreement should be in writing and signed by both parties. It should contain at least the following obligations for the processor:

i) to treat personal data only according to the instructions of the business;
ii) to treat personal data only for the purposes outlined by the business;
iii) to implement security measures in accordance with the law, and other applicable provisions;
iv) to keep the personal data to be processed confidential;
v) to delete all personal data processed once the legal relationship with the business has ended, or when the instructions of the business have been carried out, provided there is no legal provision that requires the preservation of the personal data; and
vi) to refrain from transferring personal data unless the business or a competent authority requires it.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

If the controller wishes to transfer any personal data to third parties, whether domestic or foreign, it must obtain the data subject's informed consent for such data transfer in advance of any transfer, by means of a Privacy Notice.

According to Article 37 of the FLPPIPPE, consent is not necessary in the following circumstances:

- When the transfer is expressly allowed by the Law.
- When personal data is already available in the public domain.
- When personal data has been disassociated from any identifiable parameters.
- When the collection of personal data is required for the compliance with obligations pursuant to a legal relationship between the data subject and the data owner.
- When there is an emergency that jeopardises the data subject.
- When the collection of personal data is indispensable for medical attention and/or diagnosis, for rendering sanitary assistance, for medical treatment or sanitary services. This applies provided that the data subject is not in a condition to give consent, and provided that the data collection is performed by a person subject to legal professional privilege.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

5.2 How do such considerations change depending on the nature of the entities involved?

Mexican law does not really establish different considerations regardless of whether the collecting, processing and sharing of personal information is carried out by a private entity or an entity from the public administration.

The key principle is that the basis for the lawful collection and processing of personal information is the consent, and when dealing with sensitive personal information the consent must be obtained in writing (digital means accepted).

5.3 Which key regulatory requirements apply when it comes to sharing data?

In general, Mexican data protection laws follow international correlative laws, directives and statues, and therefore have similar principles, scopes of regulation and provisions.

The key regulatory requirement consists of bearing in mind that a consumer's health information constitutes sensitive personal information and therefore, previous consent in writing is necessary for its sharing.

If the information to be shared is not personal information or has gone through an anonymisation process, or was obtained from any public source, then so far there are no restrictions for its sharing.

6 Intellectual Property

6.1 What is the scope of patent protection?

The criteria for patentability are:

- patentable subject matter (i.e. subject matter that is eligible for patent protection);
- novelty (i.e. anything not found in the prior art);
- inventive step (i.e. results of a creative process which are not obvious from the prior art to a person skilled in the art); and
- industrial application (i.e. the possibility of an invention being produced or used in any branch of economic activity).

According to Article 16 of the Industrial Property Law, the following subject matter is not patentable:

- essentially biological processes for obtaining, reproducing and propagating plants and animals;
- biological and genetic material as found in nature;
- animal breeds;
- the human body and the living matter constituting it; and
- plant varieties.

Further, Article 19 of the Industrial Property Law states that the following subject matter is **not considered an invention**:

- theoretical or scientific principles;
- discoveries that consist of making known or revealing something that already existed in nature, even though it was previously unknown;
- **diagrams, plans, rules and methods for carrying out mental processes, playing games or doing business, and mathematical methods;**
- **computer programs;**
- **methods of presenting information;**
- aesthetic creations and artistic or literary works;
- **methods of surgical, therapeutic or diagnostic treatment applicable to the human body and animals; and**
- juxtapositions of known inventions or mixtures of known products, or alteration of the use, form, dimensions or materials thereof, except where in reality they are so combined or merged that they cannot function separately or where their particular qualities or functions have been so modified as to produce an industrial result or use that is not obvious to a person skilled in the art.

Computer-readable claims are eligible for patent protection as long as the methodology and functions involved meet the patentability requirements.

6.2 What is the scope of copyright protection?

Copyright protection would be applicable for the protection of any original software used for rendering digital health services or for operating digital health devices, since Mexico opted for this sort of protection in connection with software.

A copyright certificate of registration would serve as the basis for bringing legal actions derived from the reproduction or unauthorised use of the copyrighted software.

6.3 What is the scope of trade secret protection?

Mexico does not have any national trade secret protection laws. Instead, it adheres to the provisions of Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), of which it is a signatory. Article 39 specifies that in order to qualify as a trade secret:

- The information must be secret (i.e. not generally known among, or readily accessible to persons within the circles that normally deal with the kind of information in question.
- The information has commercial value because it is secret.
- The information has been subject to reasonable steps to keep it secret, by the person lawfully in control of the information.

6.4 What are the typical results on academic technology transfer rules?

There have been some examples of positive outcomes on the development of policies for academic technology transfer processes, however, this area of law requires further development in Mexico.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Mexico does not have any specific regulation for the intellectual property protection of Software as a Medical Device.

Software as such cannot be patented in Mexico, since it falls within the prohibitions of Article 19 of the Industrial Property Law, which provides that computer programs are not considered inventions. **Nevertheless, computer-readable claims are eligible for patent protection as long as the methodology and functions involved meet the patentability requirements.**

As mentioned above, copyright protection is also available for software.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The main considerations that should be taken into account are the delimitation of tasks, rights and obligations of each party involved on the agreement. In addition, other external factors should be considered, such as regulatory requirements of the healthcare products and services, the speed of development of the field, the regulation for data collection, use, processing, and sharing, and tax and corporate compliance requirements.

7.2 What considerations apply in agreements between health care and non-health care companies?

Recently, the Mexican government approved several amendments to the Tax Law. In summary, digital health platform providers could be taxed even though the medical service itself is exempt from tax. Agreements between telemedicine providers and digital platforms can help to determine whether these entities fall within the scope of the law.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

In Mexico, the role of machine learning in digital health would be exactly the same as those observed in any other country wherein machine learning is being applied in digital health; namely, in the obtaining of more accurate and faster diagnostics and diseases detection; the development of new and better drugs and treatments, and the improved provision of medical services through digital platforms and electronic devices.

8.2 How is training data licensed?

There are no special considerations from a Mexican perspective in connection with the licensing of training data. Since this is a topic of recent discussion in Mexico, international trends and best practices are being adopted. One of the most important ones is to have the attorneys involved in the machine learning process where the training data will be used, in order to elaborate an agreement wherein it is defined who owns the data, verify the accuracy of the data and determine the licensed uses of the training data, among others.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

The ownership of inventions created by artificial intelligence has not yet been tested in Mexico. Current legislation specifies that a human inventor is required in order for an invention to be patentable. Therefore, such algorithms would not be protected under any intellectual property rights.

As artificial intelligence creates more and more inventions without active human involvement, Mexican lawmakers will need to debate and develop new laws in order to protect the inventions created.

8.4 What commercial considerations apply to licensing data for use in machine learning?

As stated above, some of the main commercial considerations to have in mind when drafting data licensing agreements are:

- The ownership of the data.
- The treatment of original and derived data.
- Conflicting interests between vendors and customers' use of the data.
- Drafting a proper and tailored definition of the training data set.
- Defining in an accurate and tailored manner the uses of the licensed data.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

As mentioned above, digital health is developing in Mexico but the laws surrounding it are yet to be decided. The rules of common civil law would apply. Digital health service providers should be diligent in checking any changes to the law to be informed about any potential liabilities in the event of adverse outcomes when using digital health technologies.

9.2 What cross-border considerations are there?

In general, the applicable regulation in Mexico concerning health products (i.e. medical devices) require marketing authorisation holders (MAH) to appoint a legal representative in Mexico (a company who has to comply with regulatory duties on behalf of the MAH):

- The local & legal representative (a company) has to be located in Mexico.
- The MAH must grant sufficient authority to the legal representative, who should have a broad scope of activities, since this representative must be able to comply with any kind of MAH's duties, such as labelling, technovigilance and/or pharmacovigilance and quality control responsibilities.

In addition, the NOM 240, which regulates technovigilance, requires the MAH of medical devices to inform of any adverse effect occurring abroad if the device involved is also commercialised in Mexico.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Mexican law regulates the processing of PII in services, applications, and infrastructure in cloud computing. That is, the external provision of computer services on-demand that involves the supply of infrastructure, platform, or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared. For these purposes, the data controller may resort to cloud computing using general contractual conditions or clauses.

These services may only be used when the provider complies at least with the following:

- it has and uses policies to protect personal data similar to the applicable principles and duties set out in the Law and these Regulations;

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- it makes subcontracting that involves information about the service that is provided transparent;
- it abstains from including conditions to providing the service that authorises or permits it to assume the ownership of the information about which the service is provided;
- it maintains confidentiality with respect to the personal data for which it provides the service; and
- it has mechanisms at least for:
  - disclosing changes in its privacy policies or conditions of the service it provides;
  - permitting the data controller to limit the type of processing of personal data for which it provides the service;
  - establishing and maintaining adequate security measures to protect the personal data for which it provides the service;
  - ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it; and
  - impeding access to personal data for those who do not have proper authority for access or in the event of a request duly made by a competent authority and informing data controller. In any case, the data controller may not use services that do not ensure the proper protection of PII.

No guidelines have yet been issued to regulate the processing of PII in cloud computing.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

The key issues that should be considered by non-healthcare companies before entering today's digital healthcare market are mainly the regulatory requirements of the healthcare products and services, the speed of development of the field, the Mexican reimbursement systems (public and private sector), the regulation for data collection, use, processing, and sharing, and tax and corporate compliance requirements.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

Digital health is a relatively new industry in which many of the businesses operating are start-ups or scale-ups. Any investor should consider the risks that could accompany such types of businesses, such as poor management structure or inadequate processes.

Another important consideration when making a decision to invest is how the market perceives digital health services. In Mexico, digital health services are still developing and therefore investment may be slow. Also, the digital health sector shifts rapidly and therefore investors must consider whether a certain company will provide long-term profits.

Finally, data security and privacy breaches can decide the success and survival of a company. In Mexico, data protection laws largely follow similar laws of other countries, and digital health service providers must follow such laws. Also, if processing or transferring data internationally, companies must ensure they comply with international laws on data protection such as the GDPR or the EU–US Privacy Shield. Any investor must be sure these laws are being fully complied with by Mexican digital health service providers before investing, to avoid any risks in losing their investment if a breach occurs.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Abraham Díaz co-chairs the Privacy and IT Industry group and has a wealth of knowledge across the IP spectrum. Abraham focuses his practice on copyright, trademarks and unfair competition, litigation, licensing and prosecution matters. He counsels clients on any IP-related matters, and handles matters involving trademarks, trade dress, product configuration, unfair competition, advertisement-related matters, false advertising, trade secrets, plant breeders' rights, vegetal varieties and Internet-related IP issues. His Internet experience includes handling domain disputes under the UDRP, as well as counselling clients concerning the development of websites and the protection of the content thereof.

He also counsels clients with regards to the correct implementation, monitoring and auditing of privacy management programs, and crisis and data breach management.

Because of his broad background, Abraham is perfectly placed to advise clients on a range of subjects and is able to assess the legal needs within this sector from a 360° standpoint.

OLIVARES Y COMPAÑIA
Pedro Luis Ogazón 17
San Ángel 01000
Ciudad de México
México

Tel: +52 55 5322 3000
Email: abraham.diaz@olivares.mx
URL: www.olivares.mx

Ingrid Ortíz is member of the Life Sciences & Pharmaceutical law and related matters, such as Digital Health at OLIVARES. Her practice is mainly focused on Intellectual Property Litigation, Regulatory and Administrative Litigation; as well as Regulatory and Compliance advisory concerning, among others Digital Health. Her main areas of practice allow her to interact with the Mexican sanitary agency, among others, the Federal Commission for Protection against Sanitary Risks (by its acronym in Spanish "COFEPRIS"), the Mexican Patent and Trademark Office (by its acronym in Spanish "IMPI"), and the Courts of law, such as the Federal Court of Tax and Administrative Affairs, the Federal District Courts and the Federal Circuit Courts.

OLIVARES Y COMPAÑIA
Pedro Luis Ogazón 17
San Ángel 01000
Ciudad de México
México

Tel: +52 55 5322 3000
Email: ingrid.ortiz@olivares.mx
URL: www.olivares.mx

Having been in business for over 50 years, OLIVARES continues its legacy of excellence in client service and attracts clients from all areas of Mexico, in addition to international clients needing counsel regarding Mexican laws, regulations and cases.

www.olivares.mx

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Saudi Arabia

Hammad & Al-Mehdar Law Firm

Suhaib Hammad

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

The Ministry of Health's Digital Health Strategy Update, defines digital health as "the cost effective and secure use of information and communication technologies and the associated cultural change it induces, to help people manage their health and well-being and transform the nature of healthcare delivery" (https://www.moh.gov.sa/en/Ministry/vro/EHealth/Documents/MoH-Digital-Health-Strategy-Update-2018.pdf).

1.2 What are the key emerging technologies in this area?

The Ministry of Health (MoH) aims to improve the efficiency and effectiveness of the healthcare sector through the use of information technology and digital transformation. Digital healthcare technologies and innovation are part of the Kingdom's "Vision 2030". The Ministry is aiming for at least 70% of the citizens to have unified digital records by 2020.

Implementation of E-health and electronic information systems has already started in a number of hospitals and organisations such as the King Faisal Specialist Hospital and Research Centre (KFSH and RC), the National Guard Health Affairs, and medical services of the army forces and university hospitals.

Additionally, a series of conferences on E-health have been held by the Saudi Association for Health Information to emphasise the importance of E-health in enhancing the quality of healthcare delivery and to explore the necessary strategies, policies, applications and infrastructure.

Telemedicine is the technology which enables physicians to provide healthcare from a distance through advanced electronic communication systems. Treatment would involve remote examination, automatic forwarding of examinations and analysts' results, exchanging expertise, conducting operations, and other medical applications which make use of computer and communications systems in transferring medical information to other locations for remote diagnosis (see E-health by Altuwaijiri).

Telemedicine was recently launched to target 69 regions in total, including Tabuk, Asir, Jazan, Northern Border, Najran, AlJouf, Al Baha, Al Qunfudhah, Hafer Albaten and Bisha (see MoH Digital Health Update).

There is a significant increase in the use of telemedicine in this area, which allows providers to offer services under the supervision of locally registered physicians on a consultancy basis.

One of the key emerging technologies includes medical devices, which are software that assist with the treatment and diagnosis of medical issues. Mobile applications such as prevention services, the provision of smart and fast diagnostics for infectious diseases, patient self-management and educational tools are some of the most important technologies that are arising. The MoH disclosed to our firm their successful projects of two major mobile applications used with patients. The first mobile application is used to facilitate the process of communicating with a physician (through text, audio call, and video call) and obtaining a diagnosis and prescription from home, such as the Cura application. The second application feeds the user's data and connects the user with a physician for an appointment at one of the registered medical facilities.

Robotics and Artificial Intelligence are also some of the important technologies developing within the area.

The key emerging technological systems in Saudi Arabia include the ERP system, EMR, CPOE, PACS, and health portals. These are all present at the King Faisal Specialist Hospital and Research Centre. The National Guard Health Affairs has also implemented the systems mentioned above and has installed advanced computer networks in all hospitals that exceed 20,000 points. Four hospitals and 60 clinics are interconnected *via* a wide area network.

EMR is an electronic healthcare information record that stores patient information with full interoperability within a health enterprise. It helps connect the work produced by different medical and technical departments. All services rendered to the patient will be stored in the patient record, which secures a more integrated and harmonious interaction between the hospital departments with a view to providing an excellent health service (see E-health by Altuwaijri).

PACS (Picture Archiving and Communication Systems) aims to replace manual medical imaging systems that depend on radiological films with a digital system that enables more than one physician to examine digital images through a computer network. This overcomes the problem of lost images, which reduces the cost of taking images multiple times (see E-health by Altuwaijri).

Moreover, the government is moving toward implementing its "Vision 2030" to improving the quality of public health indicators in the Kingdom of Saudi Arabia. This vision will be implemented through a public company named Lean that aims to offer business solutions and products to raise the efficiency of the health sector and improve the level of services provided. These services will include E-services, data analysis, and improve productivity and digital health (https://lean.sa/).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

1.3 What are the core legal issues in health care IT?

Along with confidentiality, privacy, and security, other issues include changes to the standard of care in regard to using electronic rather than paper medical records, user training, and assuring accurate information is in the medical record and provided to users. These factors affect liability which is an important legal issue when it comes to healthcare IT.

There are other unique issues involved with the use of clinical diagnosis support tools, exchange of health information across institutions, and the incorporation of genomic information into the clinical record. Informed consent for exchange of information as well as for the use of specialised tools will also be important to address.

Given the sensitive nature of healthcare information, and the high degree of dependence from health professionals on reliable records, the issues of integrity, security, privacy and confidentiality are of particular significance and must be clearly and effectively addressed by health and health-related organisations and professionals.

The intrinsically sensitive nature of patient data, along with the growing use of network computing for healthcare information processing, create the legal challenges mentioned above. The growth of off-site processing and storage of electronic health records by Application Services Providers (ASPs) adds a new dimension to those issues.

Maintaining and safeguarding the integrity and physical protection of data and systems, privacy and confidentiality of individual health information, quality of content, and the protection of consumers and online health industry commercial interests against unethical practices, are the areas of greatest concern in the implementation and use of the internet and other interactive applications in health and healthcare (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761840/).

2 Regulatory

2.1 What are the core health care regulatory schemes?

Some of the core healthcare regulatory schemes are the following:

- Private Health Institutions Law issued by Royal Decree number M/40 dated 3/11/1423H.
- Executive Regulations of Private Health Institutions Law, issued by Ministerial Decree 683151 dated 10/3/1436H.
- Executive Regulations of Health Practice Law issued by Royal Decree number M/59 dated 4/11/1426H.

2.2 What other regulatory schemes apply to digital health and health care IT?

The Telemedicine and Remote Care Centres Law, issued by the Ministry of Health, regulates digital health and healthcare IT. It outlines the services that can be offered through telemedicine, the medical conditions that can be regulated through telemedicine, and other relevant matters.

2.3 What regulatory schemes apply to consumer devices in particular?

The regulatory scheme which applies to consumer devices in particular is the Medical Devices Interim Regulation issued by the Saudi Food and Drug Authority Board of Directors, together with eight Implementing Rules adopted by the SFDA/MDS.

The Interim Regulation specifies the overall framework of the regulatory approach to allow only those medical devices that have been authorised by the SFDA to be placed on the KSA market, to ensure organisations involved in importation and distribution activities are registered with the SFDA, to ensure authorised representatives acting on behalf of overseas manufacturers are registered with the SFDA, and specifies appropriate post-marketing surveillance activities.

The eight Implementing Rules specify and refine the provisions of the Interim Regulation. As required by Article 43 of the Medical Devices Interim Regulation, each Implementing Rule specifies its application date and the application date of the provisions of the Medical Devices Interim Regulation to which it relates.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The MoH and the Saudi Food and Drug Authority (SFDA) are responsible for the overall administration of the healthcare industry in the Kingdom, while the Council of Cooperative Health Insurance oversees the insurance market.

The Ministry of Health is the lead government agency responsible for the management, planning, financing and regulating of the healthcare sector. It also undertakes the overall supervision and follow-up of healthcare related activities carried out by the private sector.

On the other hand, the Saudi Food and Drug Authority was established under the Council of Ministers resolution No. (1) dated 07/01/1424H as an independent body that directly reports to the President of the Council of Ministers. The Authority objective is to ensure the safety of food and drug for humans and animals, and the safety of biological and chemical substances as well as electronic products. The main purpose of the SFDA establishment is to regulate, oversee, and control food, drugs, and medical devices, as well as to set mandatory standard specifications thereof, whether they are imported or locally manufactured. Additionally, the SFDA is in charge of consumers' awareness on all matters related to food, drugs and medical devices and all other products and supplies.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The Law of Practising Healthcare Professionals issued on 6 December 2005 provides the rules regarding practising healthcare profession in Saudi Arabia. The Law states the requirements for licensing, duties and professional responsibility. According to the Law, a specialist panel, the "Sharia Medical Panel", was established to look into claims relating to medical malpractice. This panel is made up of both legal and medical experts to view legal disputes. Decisions arising from this panel may be appealed to the Board of Grievances within a certain time limit.

Article 34 of the Law of Practising Healthcare Professions states that the Sharia Medical Panel shall have the following jurisdiction:

a) to look into claims of medical malpractice in cases brought before it regarding private rights; and
b) to look into cases of medical malpractice, even in the absence of a claim for a private right.

The Law creates liability on malpractice of medical professionals entitling patients to claim indemnity and seek remedy.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

As discussed in question 2.3 above, the Interim Regulatory Scheme comprises the Medical Devices Interim Regulation issued by the Saudi Food and Drug Authority Board of Directors together with eight Implementing Rules adopted by the SFDA/MDS.

The SFDA has launched the Medical Devices National Registry (MDNR) for the purpose of obtaining a profile of the KSA medical device industry and establishing a database of all establishments, manufacturers, agents, and suppliers working in the field of medical devices. Enrolment is through the SFDA's official site which requires certain information and identification of the registrant (e.g. local manufacturer, importer, and distributer).

The SFDA has launched a Medical Device Establishment Licensing System (MDEL) for establishments presently involved in importation and/or distribution of medical devices on the Saudi market. The applicant has to be registered in the Medical Devices National Registry (MDNR) and shall ensure that it is able to manage appropriately the imported and/or distributed devices in relation to storage, transport, traceability, installation and the like.

The SFDA has established the National Centre for Medical Devices Reporting (NCMDR) to record, analyse and manage medical device recalls and adverse events occurring with devices during their use. The main objective is to reduce the likelihood of occurrence of incidents and/or to prevent repetition of adverse events. Authorised representatives, manufacturers, importers, distributors and users are expected to inform the SFDA about any device recalls or adverse events of which they are aware. This process applies to all medical devices placed on the market and/or in use within the KSA.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**

  Some of the issues with telehealth are payment, misdiagnosis, and widespread implementation.

  It is a big challenge to reimburse telemedicine services compared to those of in-person services. There is no guarantee of payment consistency between telemedicine and in-person healthcare. This could defeat the purpose of telemedicine to reduce healthcare costs and expand access to service as it may discourage providers from offering telehealth because there is no guarantee of comparable payment.

  The risk of misdiagnosis increases with telehealth. There is also no clear standard of care established by legislation. Misdiagnosis may increase the overall costs of healthcare, contrary to what telehealth aims to achieve, because misdiagnoses leads to wrong prescriptions and treatments.

  The challenges of widespread implementation of telehealth encompass many different areas, because "telehealth" can refer to so many different things – from robotics to telephone consultations. Some of the responsibility of implementation resides with the legal system and rests with the government. Some is institutional and rests with local hospitals and healthcare institutions; other challenges could be financial (https://healthinformatics.uic.edu/blog/challenges-facing-the-telehealth-industry).

  The challenges for implementing and adopting telemedicine in Saudi Arabia are different for each Health Care Facility (HCF) because there are different types of HCF in the Saudi healthcare system belonging to different sectors (MoH sector, military sector, private sector, etc.). Additionally, the HCFs are located in different areas: some in urban, others in rural areas. These changes make the challenges to implementing telemedicine different for each facility, seeing as each HCF will have its own motivations and expectations, business needs, etc.

  However, some issues include the following: changes in the healthcare model caused by telemedicine, in general, results in challenges that are technological, organisational, human and economic. The main challenges are problems with strategic alignment, resistance to change in the redefinition of roles, responsibilities and new skills, and lack of a business model which incorporates telemedicine in the services portfolio.

  Healthcare professionals in Saudi Arabia may be resistant to the use of telehealth. Findings demonstrate that the majority of healthcare professionals in the KFHU are interested in knowing about telehealth, but only 33.3% of health professionals in hospitals adopting telemedicine are actually implementing it.

- **Robotics**

  Medical robotics are beneficial because of their ability to perform complex surgical operations, whether directly or indirectly, such as brain, open heart and nerve surgeries through a remote robotic control system.

  Robotics have been used for medical purposes in Saudi Arabia for several purposes. One of the purposes is to allow specialised doctors to connect from Riyadh and Jeddah with patients during their pilgrimage in Madina and Makkah. According to Ministry of Health officials, medical doctors from major hospitals in Riyadh and Jeddah have been trained on using the technology.

  Robotics are useful in that they can be moved among the vast sprawling tent city of Makkah and help pilgrims without having to move them away from their accommodation during the Haj. The robot technology includes tools, such as specialised cameras to check eyes and ears, as well as cameras to inspect the skin, to enable doctors to diagnose patients and offer consultations (https://www.arabnews.com/node/1535456/saudi-arabia).

  Additionally, Saudi Arabia uses medical robotics at Johns Hopkins Aramco Healthcare (JHAH) to carry out surgeries such as a hysterectomy. JHAH's robotic surgery programme began in December 2016 when Dr. Tareq M. Al-Tartir collaborated with Dr. Mohamad Allaf. They jointly conducted the first surgeries in the Kingdom using the da Vinci Xi Robotic Surgical System. The programme has since expanded and includes gynaecological surgeries and bariatric surgery (https://www.jhah.com/en/news-events/news/robot-assisted-surgery).

  Some of the challenges are new ethical and social risks and tensions in the legal system. The use of robotics impacts privacy, human dignity and autonomy (e.g. isolation), the possibilities of human augmentation, and creates technical dependencies which can have the opposite effect of fostering learning (e.g. medicine without doctors) (https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/638391/IPOL_IDA(2019)638391_EN.pdf).

- **Wearables**

  Wearable technology in healthcare includes electronic devices that consumers can wear, like Fitbits and smartwatches, and are designed to collect the data of users' personal health and exercise.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Some of the issues with wearables is the potential sabotage of the devices themselves and the use of devices as a backdoor into networks and patient data. If wearables that monitor patient health and data are broken or stop working, this may create major issues for the patient relying on the wearable device. Inaccurate data from the wearables can have a negative consequence on the patient's health. Furthermore, lack of proper security may jeopardise the patient or user's security and data protection (https://hitconsultant.net/2019/05/29/3-major-problems-with-the-medical-device-and-wearables-market-in-2019/#.Xcf_TJLXLct).

- **Virtual Assistants (e.g. Alexa)**
  The issues here are similar to those in Artificial Intelligence. Issues such as data privacy and security are to be considered, as well as errors, and variation in the quality of the assistance provided.
  Error in dictation, high costs, challenges of adoption among healthcare professionals, and variation in the quality and security issues are the major factors that may hamper the growth of virtual assistants to a certain extent (https://www.globenewswire.com/news-release/2019/08/21/1904989/0/en/Healthcare-Virtual-Assistants-Market-worth-1-76-billion-by-2025-Exclusive-Report-by-Meticulous-Research.html).
- **Mobile Apps**
  As stated in question 1.2 above, medical mobile apps are being used in Saudi Arabia and, according to the MoH officials, they are achieving goals and increasing efficiency. One of the mobile apps discussed earlier has created more than 30,000,000 medical appointments. The other app, concerned with diagnosis and prescription from a distance, was awarded as one of the top five governmental apps.
  Some of the challenges associated with medical mobile apps in Saudi Arabia are data privacy and security and successful user experience, as well as technical challenges like managing large data on the platform. Cloud integration and compatibility with older medical systems are also a challenge.
  Cloud adoption is the main technical challenge for Mobile Application Development Services in Saudi Arabia because of security concerns about cloud platforms. Some cloud-based storage databases cannot be properly secured when it comes to maintaining patient data and information. With the upcoming data protection regulations and artificial intelligence, we believe that they will fully regulate these issues related to storing personal data.
  Modern applications face the challenges of incompatibility with old hospital systems. Old systems are not compatible with advanced healthcare applications, making it difficult for these applications to provide services to hospitals and medical centres that still operate using old technology (https://www.appsout.com/blog/which-type-of-challenges-mobile-app-development-services-in-saudi-arabia-faces-in-healthcare).
- **Software as a Medical Device**
  The same challenges apply for software as medical devices as with mobile apps. The safety and security of medical devices driven by software, the software-development processes, and the need for data collection and privacy, all offer challenges and opportunities for device regulation and clinical care (https://bioengineeringcommunity.nature.com/users/257248-william-gordon/posts/49834-challenges-and-opportunities-in-software-driven-medical-devices).
- **AI-as-a-Service**
  In terms of Saudi Arabia, Artificial Intelligence is one of the technologies which are to be focused on for the year 2020, according to the 2018 Digital Health Update issued by the Ministry of Health. One of the goals for the digital vision is for Artificial Intelligence to monitor patients virtually from their home devices, then alerts to be sent for abnormal readings and possible actions to be recommended (see the Digital Health Update 2018).
  The benefits of AI are that it can predict and diagnose disease at a faster rate than most medical professionals. It can assist in reducing workloads, lowering costs, and bettering outcomes in the delivery of administrative work, diagnosis, and treatment. AI already aids physicians in robotic-assisted procedures by providing a suggested road map and warnings throughout the process.
  Issues related to AI as a service thrive in areas such as data security, patient privacy, legal liability, and the challenges of applying AI tools in new contexts. Another challenge is the regulation of AI.
  A host of different stakeholders play key roles in overseeing and implementing these AI technologies, including hardware and software developers, clinicians, hospital administrators, and regulators. Each of these stakeholders is essential to the safe and secure diffusion of AI within healthcare delivery. Developers and clinicians must work together to carry out rigorous studies and clinical validation before using AI systems for patient care. Hospital administrators must evaluate AI in the context of developmental stages to select opportunities for adopting new technologies. Finally, regulators must continue to refine their role in legitimising and approving AI-driven tools (https://catalyst.nejm.org/health-care-ai-systems-changing-delivery).
- **IoT and Connected Devices**
  The main issues concerning the IoT and connected devices in healthcare are easing security concerns, data integrity by keeping the IoT hardware updated, technical issues like maintaining connectivity, and the government regulating this technology.
- **Natural Language Processing**
  Natural Language Processing can be used for comprehending human speech and extracting its meaning, as well as unlocking data in databases and documents by mapping out essential concepts and values and allowing physicians to use this information for decision-making and analytics. NLP can improve patient interactions with the provider, increase patient health awareness, improve care quality, and identify patients with critical care needs.
  However, some of the challenges in the application of NLP is adapting existing systems to new clinical settings. This is both time-consuming and requires a lot of effort. Some of the technical challenges in adapting the NLP system are related to assembling *corpora* and interpreting diverse linguistic content. Failure to interpret linguistic content properly can result in inaccurate results or unsatisfactory assistance from the NLP (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6080843).

3.2 What are the key issues for digital platform providers?

Digital platform providers must comply with the regulations concerning digital health, data privacy and security, as well as provide high quality medical service through these platforms. In the absence of regulation concerning specific technology, the

© Published and reproduced with kind permission by Global Legal Group Ltd, London

providers must be careful to reduce any misdiagnosis or privacy infringement resulting from the digital technologies to avoid any liability or enforcement against them.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The key issues to consider for the use of personal data are confidentiality and security. There are a number of provisions in different Saudi laws which relate to the protection of personal information. The concept is enshrined in the Saudi Basic Law of Governance issued by Royal Decree number A/91 dated 27/8/1412H. Additionally, the concept of confidentiality is preserved under Sharia, the source from which Saudi laws derive. Saudi law and Sharia cannot contradict one another.

Furthermore, there are several legislative provisions in different laws which protect the confidentiality of personal information, such as the Saudi Anti-Cyber Crime Law, E-Commerce Law and the Saudi Telecommunications Law.

Individuals are prohibited from disclosing confidential information which would jeopardise the safety and security of the country, as stated in the Penal Law on Dissemination and Disclosure of Confidential Documents and Information issued by Royal Decree number 16913/B dated 10/5/1433.

4.2 How do such considerations change depending on the nature of the entities involved?

If the entity involved is a judicial or police authority, then considerations for the use of personal data may be compromised.

Please see the answer to question 4.4 below for more detail.

4.3 Which key regulatory requirements apply?

As stated in question 4.1, the general framework is that confidentiality of sensitive and personal data must be maintained. The concept is part of both Sharia and the Saudi Basic Law of Governance.

In healthcare, the Saudi Health Information Exchange Policies applies, which is a document that contains the policies and supporting definitions that support the privacy and security aspects of the Saudi Health Information Exchange (SeHE).

The Law of Practising Healthcare Professions, issued under Royal Decree No. M/59 dated 04/11/1426H (corresponding to 04/12/2005G) and its implementing regulations (the "PHP Law") made it an obligation on all health practitioners to protect patients' data that they become aware of, except, *inter alia*, where patients' written approval is secured. Failure to commit to such provision and to the confidentiality provisions will subject the violator to disciplinary penalties and a fine, not exceeding SAR 20,000 (equivalent US$ 5,333).

The applicable regulations governing private health institutions in the Kingdom is the Private Health Institutions Law and its Executive Regulations issued under Royal Decree No. M/40 dated 03/11/1423H (corresponding to 05/01/2003G), as amended (the "PHL Regulations"). The PHL Regulations do not impose restrictions on storage registration or export of data. Also, there are no specific restrictions or requirements on collection or export of data under the PHL Regulations. This said, consent of the patient to use, store and re-distribute the data of individuals will suffice for the purpose of the PHL Regulations.

It is worth noting that while the PHL Regulations do not impose clear restrictions on storage of data, there are additional restrictions imposed by hospitals and the Ministry of Health, especially in relation to entities engaging with governmental hospitals (i.e. the King Faisal Specialist Hospital). This is because data held by governmental hospitals is subject to an additional layer of protection and may not be transferred outside the hospital's servers, which are typically within the hospital building itself.

Additional regulation includes the Electronic Transactions Law issued under the Royal Decree No. M/8 dated 8 Rabi' I-1428H (corresponding to 26 March 2007) (the "Electronic Transactions Law"), which regulates the exchange of electronic communication. The Electronic Transaction Law criminalises the use of an individual's personal information, for purposes other than certification, without obtaining the written or electronic consent of the subject person.

4.4 Do the regulations define the scope of data use?

Article 3.2 of the Saudi Health Information Exchange Policies states that "this policy applies to the Saudi Health Information Exchange, and to all individuals and organisations who have access to the Saudi Health Information Exchange managed health records, including:

- participating healthcare subscribers (PHCSs);
- their business associates;
- any subcontractors of business associates that perform functions or provide services involving the use and disclosure of PHI;
- any Saudi Health Information Exchange systems service provider; and
- any other subcontractors of the Saudi Health Information Exchange".

This policy applies to all information provided to or retrieved from the Saudi Health Information Exchange systems.

Additionally, Article 21 of the Law of Practising Healthcare Professions states that a healthcare professional shall maintain the confidentiality of information obtained in the course of his practice and may not disclose it except in the following cases:

a) If disclosure is for the following purposes:
   - Reporting a case of death resulting from a criminal act or preventing the commission of a crime; in which case, disclosure may only be made to the competent authorities.
   - Reporting communicable or epidemic diseases.
   - A professional's refuting accusations pertaining to his competence or conduct of his profession made by the patient or his family.

b) If the party concerned agrees, in writing, to disclose said information, or if such disclosure to the patient's family is beneficial to his treatment.

c) If ordered by a judicial authority.

4.5 What are the key contractual considerations?

The key contractual considerations are in regard to:

1. Consent to have access to people's confidential information.
2. The requirements for storing and using sensitive data.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

As explained in question 4.1 above, privacy and security are the key issues to consider when sharing personal data, which are regulated by the laws mentioned above. The consent to obtain confidential information must be clear.

5.2 How do such considerations change depending on the nature of the entities involved?

As demonstrated in question 4.4, there are scenarios where confidentiality can be broken. If the entities involved are police or judiciary, then there are instances demonstrated in Article 21 of the Law of Practising Healthcare Professions where confidentiality of personal data may be jeopardised.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The regulations that apply when it comes to sharing data are the following:

- Penal Law on Dissemination and Disclosure of Confidential Documents/Information issued by Royal Decree number 16913/B dated 10/5/1433.
- Penal Regulations on Dissemination and Disclosure of Confidential Documents.
- Document Records and Archives Law issued by Royal Decree M/54 dated 23/10/1409H.
- Document Archiving Regulations issued by Royal Decree 7/1379/M dated 21/7/1416H.
- The Law of Practising Healthcare Professions issued under Royal Decree No. M/59 dated 04/11/1426H.
- Saudi Health Information Exchange Policies.

The Law of Practising Healthcare Professions, issued under Royal Decree No. M/59 dated 04/11/1426H (corresponding to 04/12/2005G) and its implementing regulations (the "PHP Law") made it an obligation on all health practitioners to protect patients' data that they become aware of, except, *inter alia*, where patients' written approval is secured. Failure to commit to such provision and to the confidentiality provisions will subject the violator to disciplinary penalties and a fine, not exceeding SAR 20,000 (equivalent US$ 5,333).

Article 4.1 of the Saudi Health Information Exchange Policies states that "The purpose of this policy is to ensure that the information security is conducted in a manner that protects personal health information and supports the availability, confidentiality, integrity, and accountability of the Saudi Health Information Exchange shared clinical information".

Furthermore, provisions relating to the sanctity and safety of individuals' personal data are spread out over a number of legislative instruments. One of them is The Basic Law of Governance which broadly protects the privacy of individuals by stating that "Property, capital, and labour are basic constituents of the economic and social structure of the Kingdom. They are private rights which fulfil a social function in accordance with Islamic Sharia".

The Anti-Cyber Crime Law of 2007 prohibits the interception of data transmitted on an information network and the Telecommunications Act of 2001 outlines sanctions for breaches of privacy in the telecommunications sector.

The Electronic Transactions Law imposes certain obligations on an ISP stating that the ISP and its staff must maintain confidentiality of information obtained in the course of business.

Additionally, we recommend following General Data Protection Regulations (GDPR) standards and practices.

6 Intellectual Property

6.1 What is the scope of patent protection?

The scope and protection of patent protection is governed by the Patents, Layout Designs and Integrated Circuits, Plant Varieties and Industrial Models law, issued under Royal Decree No. M/27 dated 17 July 2004. The scope of patent protection relates to a single invention or to a group of integrated parts that form a single invention concept.

Invention can include any new article, method of manufacture, or improvement in either of them. Therefore, the invention can be a product, process or related to either. Patent protection generally extends for 20 years, from the date of filing.

6.2 What is the scope of copyright protection?

The scope of copyright protection is governed by the Saudi Copyright Law promulgated on 2003 by Royal Decree No. M/41. Scope here covers works of Saudi and non-Saudi authors published, produced, performed or displayed for the first time in Saudi Arabia. This also extends to protect the works of Saudi authors only if conducted outside Saudi Arabia for the first time.

In addition, works of broadcasting organisations and producers, i.e. sound recordings and performers, are copyright protected. Also covered are any works copyrighted pursuant to international agreements or treaties relating to copyright protection the Kingdom is a party to. Duration of copyright in Saudi law varies from 50 years' protection to life protection depending on the type and ownership of copyright.

6.3 What is the scope of trade secret protection?

The scope of protection of trade secrets is prescribed in the Regulations for the Protection of Confidential Commercial Information (Trade Secrets Regulations) issued by the Ministry of Commerce and Industry Decision No. 3218, in 2005, which vaguely defines the trade secrets as information not known in its final form or where information is not easily obtainable by those who deal in the same type of business.

The regulation also extends to protect information of commercial value so long as the rightful owner takes reasonable measures to maintain its confidentiality. What is important to note here is that the Regulations do not provide for a limit on protection duration except for information submitted to an official body or competent authority for the purpose of approval, i.e. the marketing of drugs or for chemical substances used in chemical agricultural products. In which case, a minimum protection period of five years will apply (subject to limited exceptions).

6.4 What are the typical results on academic technology transfer rules?

The Kingdom of Saudi Arabia has established a strong communication and information technology network infrastructure, capable of providing all modern services and accommodating the high data flow resulting from the use of these services and

© Published and reproduced with kind permission by Global Legal Group Ltd, London

application. The Saudi Ministry of Education has been introducing technology to the education system for health reasons to minimise the heavy weight of books to children. The ministry is also heavily encouraging innovation in schools and the use of machine learning.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

The scope of software protection has not been mentioned in the current IP laws in the Kingdom of Saudi Arabia, nor are there any specific restrictions or requirements to protect software of a medical device. However, the owner of the IP right can voluntarily register the software with the King Abdulaziz City for Science and Technology, which is the same body responsible for the registration of patent.

Having said the above, the general rule is that, in the absence of applicable legislation, Sharia principles would apply. Under Sharia principles, software components and any unique algorithms will be protected so long as it can be proven to the adequate court in case of dispute and is consistent with Sharia public order and/or public morals.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

This is not common in Saudi Arabia as most collaborative efforts in research and developments currently take place overseas. However, from a legal standpoint, the parties should set out clearly what intellectual property, know-how, and expertise they are contributing. In addition, the collaborators must agree on the ownership of the newly developed efforts and solutions by licensing the use of their existing intellectual property to the new efforts which they can also agree on how to divide the revenue generated through said efforts.

7.2 What considerations apply in agreements between health care and non-health care companies?

The considerations which apply are non-disclosure agreements, licensing agreements and/or development agreements.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

One of the goals for the digital vision is for Artificial Intelligence to monitor patients virtually from their home devices, then alerts to be sent for abnormal readings and possible actions to be recommended (see Digital Health Update 2018).

The benefits of AI are that it can predict and diagnose disease at a faster rate than most medical professionals. It can assist in reducing workloads, lowering costs, and bettering outcomes in the delivery of administrative work, diagnosis, and treatment. AI already aids physicians in robotic-assisted procedures by providing a suggested road map and warnings throughout the process.

8.2 How is training data licensed?

Training data is usually licensed by means of licensing agreements, if the owner of such data is authorised to disclose it to a third party.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

This is currently being reviewed under the new Saudi Intellectual Property Authority which was created by Royal Decree at the end of 2017, to promote the benefits of intellectual property and to build an advanced economy based on knowledge. In such absence of applicable laws, the Kingdom will adhere to international agreements or treaties relating to such protection if the Kingdom is a party to such treaty, as well as to the Sharia principles.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The rights to licensing data for use in machine learning belong solely to the data owner; and such rights can be assigned with or without consideration. However, the granting of a licence does not prevent the data owner from utilising the data or from granting a licence on the same data to another person, unless otherwise restricted in the original licence agreement. The licensee may not assign the rights and privileges conferred on him, unless his ability to do so is expressly stipulated in the licence agreement.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Some of the liability will be a penal obligation on the unfair use of the data, not obtaining consent of the data owner, or a leak or sharing of such data without the data subject consent.

9.2 What cross-border considerations are there?

When dealing with digital health on cross-border biases, a special consideration needs to be sought in relation to the applicable regulations that permits foreign (non-GCC) persons to engage-in the Kingdom of Saudi Arabia border. The best way to address this is by consulting the Saudi Arabian Foreign Investment Authority ("SAGIA") which is the licensing body of foreign persons/entity. SAGIA ensures that any activity to be carried out in the Kingdom, does not fall within the negative list which is restricted for Saudi ownership only.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

There is no current regulation that tackles this issue in particular, however, we anticipate key issues to be: the level of protection over the data shared in the cloud; and the obligation of the cloud/service provider and the digital city to protect such data.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

There are no existing regulations or rules that discuss this issue, however, we anticipate the following issues for non-health-care companies: ownership and control over the data; software licence and application ownership; and rights to amend over them.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

Key issues for venture capital and private equity firms would concern the stability of the digital platform, size of the clients, and scope of services provided to healthcare.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Suhaib Hammad joined Hammad & Al-Mehdar Law Firm in 2009. He earned his LL.B. from IIU Malaysia and his LL.M. from the University of Miami, specialising in International Business Law.
As a Partner, Suhaib leads the Commercial and Intellectual Property practice, focusing on ICT, TMT and Life Sciences. In addition, Suhaib was placed on secondment with the corporate and commercial team at Simmons & Simmons in their Dubai and London offices, and has worked on leading cross-border transactions. His experience includes advising major international telecoms and healthcare companies on Saudi regulations in relation to formation and operation. Suhaib was also awarded a Client Choice Award by Lexology for the year 2019. The firm was recognised as the best Mergers & Acquisitions law firm for the years 2017 and 2018 by the IFN Law Awards, and has been honourably mentioned as a Tier 1 Firm in *The Legal 500* 2017 for Banking & Finance Transactions.

Hammad & Al-Mehdar Law Firm
Level 12, Office 1209
King Road Tower
King Abdulaziz Road
Jeddah
Saudi Arabia

Tel: +966 920004 626
Email: suhaib.hammad@hmco.com.sa
URL: www.hmco.com.sa

Hammad & Al-Mehdar Law Firm was founded in 1983 in Jeddah, Saudi Arabia, and has grown to become a prominent private practice Saudi firm in the Kingdom and the GCC. The law firm boasts a leading local presence supported by international capabilities.
Hammad & Al-Mehdar provides a full suite of business and corporate legal services in all major areas of Saudi law, working on cutting-edge, complex and high-value transactions and disputes.
Headquartered in Jeddah, Hammad & Al-Mehdar's growth story is one of trade, innovation and technology in the Kingdom's private sector. Hammad & Al-Mehdar maintains a strong specialisation in servicing privately held businesses, with unrivalled expertise in business and transaction structuring, private construction works, commercial, intellectual property, corporate governance, and regulatory advisory services.

www.hmco.com.sa

HAMMAD & AL-MEHDAR
LAW FIRM

© Published and reproduced with kind permission by Global Legal Group Ltd, London

South Africa


Christoff Pienaar


Nikita Kekana

Cliffe Dekker Hofmeyr

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

The Department of Health in South Africa has published the National Digital Health Strategy for South Africa 2019–2024 ("**SA Health Strategy**"). In terms of the SA Health Strategy, digital health is defined as the use of information and communications technology for health to do things such as treat patients, pursue research, educate students, track disease and monitor public health.

1.2 What are the key emerging technologies in this area?

One key trend in South Africa is the use of 3D printers in the medical sector. For instance, at the Steve Biko Academic Hospital, doctors completed the world's first middle ear transplant using 3D-printed middle ear bones.

The use of robotics is also being introduced to surgery within South Africa. Africa's first full knee replacement operation using a robotic arm-assisted surgery system was conducted in South Africa. More and more physicians are getting qualified to perform robotic surgeries.

The South African National Blood Service has developed its own drones for the transportation of blood.

1.3 What are the core legal issues in health care IT?

The core legal issues in healthcare IT in South Africa are data protection, ownership of the digital health technology (especially copyright issues concerning big data and artificial intelligence), regulation (particularly the health and safety in using digital health technology) and dispute resolution.

With the advancement of technology, data including big data is now being analysed and used to develop medical technologies and services. So, there is an increased focus on data protection and regulating the processing of personal information.

With the development of many different types of technology, the determination of usage rights, licensing rights and ownership of such technology is critical.

There is pressure to keep up with the developmental trends in the digital health sector and regulate this sector in a way that protects the safety of patients without stifling innovation.

There is also a need to resolve disputes in this sector swiftly and efficiently so as not to jeopardise access to the technology but at the same time uphold fair judicial process and the rule of law.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The core pieces of legislation applicable in the health sector are the National Health Act 61 of 2003, the Medicines and Related Substances Act 101 of 1965, the Medicines and Related Substances Amendment Act, 14 of 2015 and the Health Professions Act No. 56 of 1974.

2.2 What other regulatory schemes apply to digital health and health care IT?

The Protection of Personal Information Act 4 of 2013 is the core legislation dealing with data protection in South Africa and is key to the digital health sector. The Information Regulator is the responsible regulatory authority.

2.3 What regulatory schemes apply to consumer devices in particular?

The Consumer Protection Act 68 of 2008 ("**CPA**") and aspects of the Electronic Transactions and Communications Act 25 of 2002 are the main pieces of legislation that apply to consumers and consumer devices. The CPA has the following regulatory bodies: the National Consumer Commission; Consumer Goods and Services Ombud; and National Consumer Tribunal, who all help enforce consumer protection, consumer rights and resolve disputes in South Africa.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

There are the following principal regulatory authorities:

The South African Nursing Council ("**SANC**") who are responsible for establishing, improving and controlling the nursing practice in South Africa and standardising nursing education and training.

The Healthcare Professions of South Africa ("**HPCSA**") which is mandated to promote health within South Africa, determine the standards of professional education and training, and set and maintain standards of ethical and professional practice of healthcare professionals in South Africa.

The South African Pharmacy Council which is an independent, self-funded, statutory body mandated in terms of the Pharmacy Act, 1974 (Act 53 of 1974) that regulates the pharmacy

© Published and reproduced with kind permission by Global Legal Group Ltd, London

profession in South Africa and is authorised to register pharmacy professionals and pharmacies, control pharmaceutical education, and ensure good pharmacy practice.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The provision, manufacturing and wholesaling of medical substances and medical devices is carefully legislated and overseen by the South African Health Products Regulatory Authority. Medical practitioners, including those that may operate online, need to be properly qualified and registered with the Healthcare Professions of South Africa.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

The core legislation that applies is the Medicines and Related Substances Act, 1965 (Act 101 of 1965) and the GN 1515 of 9 December 2016 – regulations relating to Medical Devices and *In Vitro* Diagnostic Medical Devices (IVDS). A person wishing to manufacture, import, export, distribute or wholesale software as a medical device needs to obtain the requisite licensing and authorisations from the Medicines Control Council.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

For all of the digital technologies, data protection, including security and prevention of unauthorised disclosure or access, is a fundamental issue that needs to be considered.

- **Telehealth**
  When providing telehealth solutions, companies need to ensure that information is communicated clearly and concisely so that any advice given is not misconstrued. South Africa has 11 official languages, so part of this requirement also includes communicating to end-users where possible in their own language. There also needs to be the necessary disclaimers to limit liability of the telehealth provider in relation to any suggestion given on the app.
- **Robotics**
  The ownership of both the software and hardware of the robot is an issue that needs to be considered. The safety features and limitations of the robot, particularly those used in surgery, need to be determined to avoid the issue of medical negligence claims brought against the relevant medical practitioner.
- **Wearables**
  For wearables, an issue that arises is the lack of transparency and clear communication on what data is being harvested from data subjects and the purpose for which this data is processed. Making even deidentified personal information available, such as the running routes used, could jeopardise the safety of data subjects and make them targets of criminal activity and theft if their ordinary running routes are deserted. Another issue is the possible hacking of wearables and this having severe adverse negative effects. For instance, if a wearable is used to distribute medication into a data subject and this device is hacked, it could be used to cause an overdose of medication in that person.
- **Virtual Assistants (e.g. Alexa)**
  An important aspect of healthcare is the human interaction aspect, so the issue is ensuring that virtual assistants are appropriately programmed to provide appropriate and sympathetic responses and also apply machine learning so that with each interaction, the software gets better.
- **Mobile Apps**
  Important issues for mobile apps include developing an app that is fit for purpose and ensuring that it is appropriately maintained and where necessary, upgraded. The storage and location of the mobile app's software is also an important aspect.
- **Software as a Medical Device**
  An important aspect is that the medical practitioner utilising the device is properly trained to operate the device as they would face medical negligence claims if the software was not used properly and injured a patient. Another issue is determining the licensing/ownership rights in the device.
- **AI-as-a-Service**
  The important issues to consider here are the parameters of the AI licence and also agreeing to liability exposure should the AI device cause personal injury.
- **IoT and Connected Devices**
  Anything that is connected to the internet is vulnerable to hacking so the issues are ensuring that the technology is properly protected against malware, viruses and hacking and that the technology is easily and regularly updated. It is also important to ensure that connected devices are compatible with each other and remain so even when each device is updated. This is especially important in the medical industry where devices could be needed for life-saving measures. For instance, one device may be monitoring the quantity of a particular medication currently in stock and the other device may be triggered and be responsible for ordering more medication when the stock levels reach a certain level.
- **Natural Language Processing**
  An important issue to consider with these technologies is that they are only useful if they receive enough training data and are able to further develop through machine learning to fulfil their function. When these technologies are used as chatbots, they need to be able to offer natural responses, as an important aspect of medical treatment is currently the human interaction and patients feeling heard and listened to.

3.2 What are the key issues for digital platform providers?

Digital platform providers should be aware of at least the general categories of data and software that will be used on these platforms, the level of security needed and how often this needs to be updated to limit its exposure to hackers and other unauthorised disclosure.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

When using personal data in the digital health space, two key issues include the consideration and adherence to the regulatory requirements, laid out by the Protection of Personal Information

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Act 4 of 2013 ("**POPI**"), and the importance of protecting the confidentiality of the data and securing it from data breaches as health data is generally very sensitive in nature and disclosure of such data can cause very severe reputational damage, as well as having legal ramifications.

4.2 How do such considerations change depending on the nature of the entities involved?

For the most part, it is subject matter, i.e. the type of personal information used rather than the entities, that should be considered when processing personal data in the digital health sector.

However, POPI does distinguish between responsible parties and operators.

A responsible party is the person that determines how personal information is processed and an operator is the person who processes the personal information on behalf of the responsible party.

If an entity is considered a responsible party, then POPI directly applies to that entity and non-compliance of POPI can result in fees and penalties; where as if an entity is an operator then, provided that such entity does not exceed its contractual mandate with the responsible party, POPI only applies indirectly to it and the operator's exposure is limited to what it has agreed to in its contractual mandate with the responsible party.

4.3 Which key regulatory requirements apply?

POPI is the primary data protection legislation in South Africa. Whilst POPI has been promulgated into law, its substantive provisions are not yet in effect. The President of South Africa needs to determine the full commencement date of POPI but, as an information regulator has been appointed and draft regulations drafted, this is likely to be imminent.

Personal information is essentially any information that can be used to identify a person. A data subject is the person to whom the personal information relates.

In terms of POPI, personal information about a person's health or sex life and ethnic origin is considered special personal information and the processing of special personal information is prohibited unless one of the listed exceptions applies, such as where the data subject consents to the processing.

It is vital therefore in the digital health sector for businesses to focus on obtaining the consent of data subjects when they process special personal information.

Another important issue that digital health businesses ought to consider when processing personal information is that the use of the personal information must be for a specific purpose and the general rule is that personal information should be obtained directly from the data subject.

4.4 Do the regulations define the scope of data use?

The use of personal data must only be for a specific purpose that is adequate, relevant and the processing of such data must not be excessive. Furthermore, the use of the data must be lawful and be used in a reasonable manner that does not infringe the privacy of the data subject.

4.5 What are the key contractual considerations?

When contracting, it is important to identify who is the responsible party and who is an operator under POPI, where and how the data will be stored and whether or not the personal data is being transferred outside of South Africa. A responsible party must ensure that its suppliers who would be operators under POPI are contractually bound to comply with the principles and requirements of POPI.

When contracting with data subjects the purpose for which the personal information is used must be clearly stated and where consent is relied upon for the processing of the personal information, this must be expressed in specific and unequivocal terms by the data subjects.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The identity of the person which the personal data shares is of critical importance and whether or not the personal data has been deidentified is a key consideration when sharing personal data.

Generally, if regulatory, court of law or the data subject themselves request personal data then the personal data may be shared. Furthermore, if personal data has been deidentified to an extent that the personal data cannot be reidentified, then that personal data can be freely shared unless protected by a confidentiality clause.

Deidentification and the sharing of the general findings and analytics of big data sets is often critical in the medical health space as it enables entities to commercialise data within its possession and make public importance research results.

5.2 How do such considerations change depending on the nature of the entities involved?

Under POPI, it is the responsible party who determines the nature and extent of processing personal information, thus it is this party who can determine within the bounds of the law who to share the data with. An operator is mandated to process personal information on behalf of the responsible party, so this entity cannot determine who to share personal information with.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Under POPI, a responsible party is required to keep personal information confidential. This means that, generally, data containing personal information cannot be shared with third parties.

Moreover, under POPI, the sharing of personal information would in most instances amount to further processing which is only possible if it is in accordance with or compatible with the purpose for which it was collected. This would typically not be the case when the data is shared, especially where the data is sold to a third party for advertising purposes.

Importantly, in the digital health sector, a significant portion of the data is personal information about a patient's health or sex life. As mentioned in our response to question 4.3, the general rule is that the processing of this type of data (which includes the sharing of data) is prohibited unless an exception applies, such as the data subject consenting to the data sharing.

Another instance where health or sexual life personal information could be shared is within a healthcare facility or between medical practitioners where this processing (sharing) is necessary for the proper treatment and care of the data subject. By

© Published and reproduced with kind permission by Global Legal Group Ltd, London

way of example, paramedics could share with a surgeon, about to perform emergency robotic surgery, details about the patient's current medical conditions.

It is worth noting that anonymised data where the personal information has been completely deidentified, can generally be shared with others, unless it is protected by a confidentiality agreement or similar undertaking.

6 Intellectual Property

6.1 What is the scope of patent protection?

In South Africa a patent is an exclusive right granted for an invention, which is a product or a process that provides a new way of doing something or offers a new technical solution to a problem. Patents can last up to 20 years under South African Law.

South African Law provides protection for patents registered with the Companies and Intellectual Property Commission ("**CIPC**") and South Africa is also a party state to the Patent Cooperation Treaty ("**PCT**") which is an agreement for international co-operation in the field of patents.

6.2 What is the scope of copyright protection?

Copyright in South Africa is regulated by the Copyright Act 98 of 1978 ("**Copyright Act**") and automatically subsists in original works, eligible for protection, created by a qualified person or which are first published in South Africa or another country to which protection is extended. The Copyright Act contains a clear description of the various works that are capable of copyright protection. These various works include literary works, cinematographic films, musical and artistic works and computer programs. Certain exclusive rights are vested in the owner of the copyrightable work, including the right to reproduce, publish or make an adaptation of the work in question. Persons can co-own a copyrighted work.

6.3 What is the scope of trade secret protection?

Trade secrets are not protected in terms of legislation but under the common law as long as they are kept secret and confidential and not disclosed to the public. It is possible to interdict a person from disclosing such secrets.

6.4 What are the typical results on academic technology transfer rules?

In South Africa there is the Intellectual Property Rights from Publicly Financed Research and Development Act 51 of 2008 ("**IPR Act**"). Under the IPR Act, if intellectual property is created with public funds then the public university or research institution involved in the development or commission of the intellectual property shall own the intellectual property no matter what is agreed between the parties.

The IPR Act also enables these institutions to receive subsidies and funding from public funds. The IPR Act also restricts what public institutions can do with its intellectual property. For instance, the intellectual property cannot be assigned without following the guidelines given by the National Intellectual Property Management Office ("**NIPMO**") and also notifying the NIPMO.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Software as a Medical Device would be granted protection as a computer program under the Copyright Act 98 of 1978 ("**Copyright Act**"). An owner of the Software as a Medical Device has the exclusive right to use, copy, license and dispose of the device.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

It is important to establish and agree beforehand what the ownership structure in the improvements shall be and also what each party's exposure and liability is under the collaboration.

7.2 What considerations apply in agreements between health care and non-health care companies?

It is crucial to consider what type of data is being processed under the agreement and whether personal information is processed, and if personal information is processed, then adequate data protection clauses must be included. It is also critical to determine each party's exposure and liability, particularly to third parties like data subjects if the data is unlawfully accessed.

Both entities must also ensure that the other party has the requisite expertise and authorisations to fulfil their obligations. For instance, if a hospital partners with a software developer to jointly create and own an app that provides post-hospital advice to outgoing patients then it is important that the hospital ensures that the software developer has the capabilities to develop the app and provide the necessary security safeguards. The software developer would want to ensure that the hospital is appropriately registered, the advice that is provided on the app has been properly vetted by registered and qualified medical professionals and any personal information shared is only shared where the patient has consent to the data being processed and used on the app.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning is playing an increasingly important role in digital health as it is a useful tool to constantly improve digital health solutions. For instance, in robotic surgery, machine learning can be used to ensure that the robots used learn from each surgery performed, thereby making them more effective and safer with every surgery.

One of South Africa's medical insurance providers uses AI chatbots to engage with customers on its website and help customers find the information that they need on the website. Customers can provide feedback on whether or not the information provided was useful/relevant. By utilising machine learning, these chatbots can learn which responses are appropriate for which queries based upon the customers' response, thereby improving customer satisfaction and becoming more useful to the insurer.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

8.2 How is training data licensed?

Techopedia.com defines that, "the training data is an initial set of data used to help a program understand how to apply technologies like neural networks to learn and produce sophisticated results".

In South Africa, there are a few ways in which training data is acquired. If possible, data in the public domain or already in developer's possession is used to develop the program, or a developer may offer to develop software for a client or clients and then use the clients' data as training data to build and improve the computer program.

It is also possible to "license" the training data by asking for individuals to provide it voluntarily or for some kind of compensation, although this approach is in our view less frequently used.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Algorithms are categorised as a "computer program" under the Copyright Act.

The general rule is that ownership of original work shall vest in the author, or in the case of joint authorship, in the co-authors of the work. It is therefore critical to identify who the author is. In respect of a computer program, the author is the person who exercised control over the making of the computer program. Where the work is created in the course and scope of employment (whether under a contract of service or apprenticeship), the employer will hold the copyright. Where a computer program has been commissioned, the person commissioning the work would be the author.

Where this algorithm is thereafter further improved by machine learning without active human involvement, then the owner of the algorithm would remain the person who initially exercised control over the making of the algorithm as only natural and juristic persons such as companies can acquire ownership rights and not machines.

Furthermore, even if the algorithm is improved and altered to a large extent without further human involvement that it is no longer considered the original but an adaption of the algorithm, the adaptions are also under copyright law and are considered to be owned by the author.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The most important considerations are how the licensor will be paid or otherwise compensated and agreeing who will own the analysis of the data. The source of the data is also important as, if the data contains personal information, then it is also important that the data subjects whose personal information is being processed have consented to its use in machine learning or there is another legal justification for processing this data.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Under South African law, parties are typically liable for the legal consequences that arise out of their negligence or fault.

In limited circumstances, parties may also be held strictly liable. A common example of this is vicarious liability where an employer shall be held liable for its employees' delicts (torts) that are performed within the course and scope of their employment. A common instance where strict liability will apply is in contracts involving consumers. Where a client is a natural person or small juristic person, they may also be able to hold both the service provider and developer of digital health technology liable under the Consumer Protection Act where such technology is unsafe, defective or of poor quality. This is because the producer, importer, distributor and retailer are all deemed to include an implied warranty of quality under the Consumer Protection Act. The Consumer Protection Act also contains a similar right to quality services for a consumer.

9.2 What cross-border considerations are there?

Under South African law, an entity may not export capital including intellectual property outside of South Africa without first obtaining approval from the Financial Surveillance Department of the South African Reserve Bank ("**SARB**") or an authorised dealer, where SARB has delegated its power to authorise the export of capital to that authorised dealer.

This means that if an entity has invented a digital health app/software or other asset in South Africa and wishes to expand into other countries, sell or licence the software to a foreign entity, it can only do so if it obtains the authority of SARB under the Exchange Control Regulations.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Medical data of data subjects is considered special personal information under POPIA, thus the processing of medical data, including storage on the cloud, is only allowed in limited circumstances such as where the data subjects have consented to such data processing.

Furthermore, often cloud-based providers' servers are located outside of South Africa, thus it is critical for the cross-border transfer to be lawful under POPIA.

A cloud provider is considered a service provider of a digital health entity thus, it is important for there to be proper agreements in place that protect the digital health entity's data and guarantees the security and confidentiality of medical data of any data subjects.

Furthermore, because of the sensitive nature of patient-linked digital health data, to avoid data breaches and irreparable reputational damage, it is critical for entities in this sector to partner with reputable cloud service providers when providing cloud-based health services.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Non-healthcare companies need to properly analyse compliance and regulation issues as this is a regulated sector and so, in many instances, licences and other authorisations are required to conduct their business. These companies also need to acknowledge that there are already a few big players from hospital groups to medical insurers in the medical industry that are driving

© Published and reproduced with kind permission by Global Legal Group Ltd, London

innovation in order to maintain their market share and remain relevant. This means that before entering the market, it is critical for new entrants to properly identify gaps in the market and develop a customer-centric brand identity.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

It is critical for venture capital and private equity firms to conduct comprehensive due diligence to determine whether the digital health ventures' intellectual property rights are properly protected and that the ventures actually own the digital healthcare technology that they are utilising and developing. Depending on the nature of the venture, it is also important to ensure that the entity is properly licensed and has the necessary authorisations to conduct its business.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Christoff Pienaar is a Director and the National Head of Technology, Media & Telecommunications at Cliffe Dekker Hofmeyr. He advises on commercial, information technology and intellectual property law. He specialises in information technology and commercial matters and has particular expertise in payment systems, technology outsourcing, business process outsourcing, systems integration, hardware acquisitions and maintenance, IT consultancy services, managed services, disaster recovery services, software development and software licensing and support transactions. Christoff also advises on general commercial and intellectual property issues across a diverse range of industry sectors, especially financial services.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town
South Africa

Tel: +27 21 481 6300
Email: christoff.pienaar@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Nikita Kekana is an Associate in Cliffe Dekker Hofmeyr's Technology, Media & Telecommunications practice. Nikita specialises in commercial, information technology, intellectual property and data protection law. Nikita also has a keen interest in artificial intelligence, machine learning and big data.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town
South Africa

Tel: +27 21 481 6300
Email: nikita.kekana@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

At Cliffe Dekker Hofmeyr (CDH) we believe the right partnership can lead to great things. The partnerships we cherish and value most are those we have forged through time and experience with our clients and, of course, our people. We are a full-service law firm – one of the largest business law firms in South Africa, with more than 350 lawyers and a track record spanning 165 years. We are able to provide experienced legal support and an authentic knowledge-based and cost-effective legal service for clients looking to do business in key markets across Africa.

Our Africa practice brings together the resources and expertise of leading business law firms across the continent that have direct experience acting for governments, state agencies and multinational organisations. This combined experience across the continent produces an extensive African capability. We also partner with other professional disciplines such as audit, business consulting or corporate finance disciplines to provide a seamless and integrated solution for projects that have a multi-disciplinary dimension. We focus on a number of key sectors which are active and thriving in Africa, including M&A's, mining and minerals, telecommunications, energy, oil and gas, banking and finance, projects and infrastructure, hospitality and leisure and arbitration.

www.cliffedekkerhofmeyr.com

CDH
CLIFFE DEKKER HOFMEYR

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Spain

Baker McKenzie

Montserrat Llopart

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no formal or legal definition of digital health in Spain. According to the *Fundación Tecnología y Salud*, a foundation set up by the Spanish Federation of Healthcare Technology Companies (FENIN), digital health refers to the set of Information and Communication Technologies used in a medical setting in areas related to the prevention, diagnosis, treatment, monitoring and management of health, acting as an agent of change that enables cost savings and improves efficiency.

1.2 What are the key emerging technologies in this area?

The health system is currently focusing on the development of virtual reality, artificial intelligence and robotics as the key emerging technologies.

Telehealth is increasingly taking hold and making interactive, real-time communication between patients and health professionals common-place, avoiding the need for face-to-face medical visits.

1.3 What are the core legal issues in health care IT?

The core legal issues are data privacy, quality of data, cybersecurity and the interoperability of IT systems. Regulatory issues and financing are also key for the development of healthcare IT.

2 Regulatory

2.1 What are the core health care regulatory schemes?

Royal Legislative Decree 1/2015, of 24 July 2015, approving the revised text of the Law 29/2006, of 26 July 2006 on Guarantees and the Rational Use of Medicines and Medical Devices ("RLD 1/2015") establishes the general framework of the regulation of medicinal products and medical devices in Spain.

- Royal Decree 1591/2009 of 16 October 2009, on medical devices.
- Royal Decree 1616/2009 of 26 October 2009, on active implantable medical devices.
- Royal Decree 1662/2000 of 29 September 2000, on *in vitro* diagnostic medical devices.
- Regulation (EU) 2017/745 on medical devices is applicable as of 26 May 2020.
- Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices is applicable as of 26 May 2022.
- Catalonia: Guide for Advertising of Medical Devices to the General Public of January 2017.

2.2 What other regulatory schemes apply to digital health and health care IT?

Other regulatory schemes are as follows:

- The General Data Protection Regulation (EU) 2016/679 (GDPR).
- Law 3/2018 of 5 December on Data Protection and Guarantee of Digital Rights.
- Law 34/2002 on Information society services and electronic commerce.
- Royal Decree 3/2010, of 8 January 2010, regulating the National Security Framework in the field of eGovernment.

2.3 What regulatory schemes apply to consumer devices in particular?

Regulatory schemes that apply to consumer devices are as follows:

- Royal Legislative Decree 1/2007 of 16 November, approving the revised text of the general law for the protection of consumers and users (GLPCU).
- Law 22/1994 on product liability, implementing Directive 85/374/EEC.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The Ministry of Health, Consumer Affairs and Social Services is responsible for the financing of medicines and medical devices and establishes the framework for the provision of health services. It is also responsible for consumer protection legislation.

The Spanish Agency for Medicines and Medical Devices (*Agencia Española de Medicamentos y Productos Sanitarios*) is attached to the Ministry of Health. It regulates and supervises the whole lifecycle of medicines and medical devices, from R&D activities to recalls and market vigilance, including authorisations, promotion and distribution activities.

The regional authorities (*comunidades autónomas*) are responsible for the provision of healthcare services, for the supervision of promotional activities and for consumer protection.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

The Spanish Data Protection Agency (*Agencia Española de Protección de Datos*) is the national supervisory authority under the GDPR and ensures that data privacy principles and regulations are respected.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The key areas of enforcement are as follows:

- Regulatory authorities' actions against digital health and healthcare IT that meet the definition of medical devices but have not sought or obtained the requisite authorisation (CE mark).
- The Spanish Data Protection Agency actions in the event of breaches of data protection legislation and data security.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Software that qualifies as a medical device must follow the provisions relating to medical devices, which vary depending on the kind of medical device:

- Royal Decree 1591/2009 of 16 October 2009, on medical devices.
- Royal Decree 1616/2009 of 26 October 2009, on active implantable medical devices.
- Royal Decree 1662/2000 of 29 September 2000, on *in vitro* diagnostic medical devices.

Once the transitional periods end, EU Regulations 2017/745 and 2017/746 shall apply and it is expected that the Spanish Royal Decrees will be updated.

The European Commission has issued guidelines on the classification of medical devices (MEDDEV Guidelines) and, in particular, on the Qualification and Classification of stand-alone software used in healthcare.

Solutions developed for the public administration will be checked to ensure that the security standards required of the public administration are met.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  As health data are considered special categories of personal data, data minimisation and data security are important. To the extent digital health technologies are stored on clouds outside of the European Economic Area, appropriate safeguards must be put in place.
  The Spanish deontological code of physicians is still very restrictive as regards telehealth activities. However, the national health service actively promotes telehealth as a way of optimising resources by reducing the need for face-to-face visits.
- **Robotics**
  The three core issues are security, cross-border remote control and liability. Avoiding the risk of hacking is critical. Cross-border remote control raises issues relating to differences in the qualifications of the persons located outside of Spain controlling robotic devices. Finally, it may become difficult to determine whether product defects or incorrect use are to blame when loss or damage occurs.
- **Wearables**
  The core issues are the reliability of data, privacy concerns and data security. To the extent that apps track medical conditions, liability issues may also arise.
- **Virtual Assistants (e.g. Alexa)**
  The core issues are first data security and the risk of cyber-attacks and then the reliability of data, together with privacy concerns.
- **Mobile Apps**
  The same issues apply as for wearables – see above.
- **Software as a Medical Device**
  Software that will meet the definition of medical devices needs to be developed according to the requirements set out in medical device regulations in order to obtain the CE mark.
- **AI-as-a-Service**
  The need for a large volume of data, the quality of that data and the risk of bias. The application of data minimisation principles (anonymisation, pseudonymisation), and data security. The analysis of medical images is an area of growing potential, with data quality and security being major issues.
- **IoT and Connected Devices**
  As of today, the greatest risks are cyberattacks, data security, the value and reliability of the data obtained and privacy issues. Interoperability with healthcare providers' IT systems also needs to be addressed.
  Virtual reality, augmented reality and mixed reality, with their potential for treating patients and affecting their behaviour, may pose additional security and regulatory issues.
- **Natural Language Processing**
  The existence of various official languages in Spain, some spoken by small populations. Availability of digital health technologies in several of those languages may be key to their adoption by some regional healthcare authorities.

3.2 What are the key issues for digital platform providers?

The key issues for digital platform providers are as follows:

- Interoperability of digital platforms with apps, wearables, IoT, medical devices and other digital healthcare technologies without compromising the integrity of the platforms.
- Market access issues due to the need of validation before having connection to public healthcare IT systems.
- Business models that favour the creation of value and potential savings for healthcare providers and sustainable financing models.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The main issue to consider is that genetic data, biometric data uniquely identifying natural persons, and health data are considered to be special categories of personal data, in accordance to Article 9 of the GDPR. The GPDR prohibits the processing of special categories of personal data. However, there are some exceptions, such as the explicit consent of the data subject, which is explained further in question 4.2.

The first step when using personal health-related data is to clearly define for which purposes the personal data will be used,

© Published and reproduced with kind permission by Global Legal Group Ltd, London

in order to check if any of the exceptions foreseen in Article 9 of the GDPR apply and to be compliant with the transparency principle. In this regard, it should be borne in mind that usually it will be necessary to collect the explicit consent of the data subject to process personal data concerning health and that the personal data collected cannot be used for a purpose other than that for which the data subject gave their consent.

Operators are sometimes reluctant to clearly limit the purposes for which personal data is collected and to provide transparent and granular information on how and by whom personal data is going to be processed. The reason is that operators want to preserve the possibility of extending the types of processing in the future to purposes that they may not have foreseen at the outset or that have appeared with the evolution of the market. However, this practice goes against the transparency principles of the GDPR, as well as the obligations of privacy by design and should, in consequence, be avoided.

4.2 How do such considerations change depending on the nature of the entities involved?

When the controller is a private entity, the legal basis required to process personal data relating to health is usually the consent of the data subject. In case of public authorities, there are certain circumstances under which they do not need the consent of the data subject in order to process his or her personal data.

In this regard, the Spanish Data Protection Agency has recognised that public authorities, unlike individuals, may process personal health data without the consent of the data subjects, if it is necessary for the performance of a task carried out in the public interest or in the exercise of public authority and as long as it has a competence conferred by law. For example, Article 41(2) of the General Public Health Law 33/2011, of 4 October 2011, establishes that public health authorities do not need to obtain the consent of the data subjects to process their personal health data, nor to transfer said data to other public health authorities, when this is strictly necessary for the protection of the population's health.

4.3 Which key regulatory requirements apply?

When using personal health-related data, appropriate safeguards are required. These include, for example: (i) to correctly identify the purposes for which personal data is going to be processed and only process personal data that is strictly necessary for the identified purposes (data minimisation); (ii) application of the privacy-by-default and privacy-by-design principles; (iii) to conduct a privacy impact assessment and analysis of the risks for the rights and freedoms of the data subjects prior to the processing of data; (iv) to guarantee the confidentiality, integrity and availability of the personal data processed; (v) to anonymise personal data or, at least, pseudonymise the same and prohibit third parties with whom personal data may be shared from reverting the pseudonymised data; (vi) to obtain separate consent for each purpose; (vii) to provide clear information to data subjects, using plain language and providing information about the identity of the data controller, and specifying whether personal data is shared and with whom and if it will be re-used and for which purposes; (viii) to design user-friendly settings options, so that data subjects can easily decide whether they want to share personal data or not; and lastly (ix) to take into account that profiling is only permitted under very specific circumstances and, if done, explicit consent of the data subject needs to be obtained.

4.4 Do the regulations define the scope of data use?

Yes, they do. The scope varies depending on the purpose of the processing:

a) Public health and biomedical research: the data subject may give their consent to the processing of their personal data for purposes of biomedical research. In this regard, it is important to note that personal data for health and biomedical research purposes can be reused when, having obtained consent for a specific purpose, the data is used for related research. In this case, controllers shall provide the information regarding the processing of the personal data under Article 13 GDPR, in an easily accessible place on the corporate website of the centre where the research or clinical study is being carried out, and, where appropriate, on the website of the sponsor, and notify the parties concerned of the existence of this information by electronic means. It is important to note that a prior favourable report from the Research Ethics Committee is required.

b) The processing of pseudonymised personal data: it is considered lawful to use pseudonymised personal data for health research, and in particular for biomedical research. However, the following requirements shall be fulfilled:
   (i) a technical and functional separation shall be made between the research team and those who perform the pseudonymisation and keep the information that makes reidentification possible; and
   (ii) the pseudonymised data may be accessible to the research team only when there is an express commitment to confidentiality and not to carry out any reidentification activity and specific security measures are adopted to prevent reidentification and access by unauthorised third parties.

   There is an exception in which reidentification of the data at the source may take place. This is when, in the course of an investigation using pseudonymised data, it becomes apparent that there is a real and specific danger to the safety or health of a person or group of persons, or a serious threat to their rights, or reidentification is required to ensure proper healthcare.

c) Situations of exceptional relevance and seriousness for public health: health authorities and public institutions with responsibilities for public health surveillance may carry out scientific studies without the consent of those concerned in situations of exceptional public health relevance and seriousness.

4.5 What are the key contractual considerations?

The key contractual considerations are as follows:

a) Privacy contractual considerations with data subjects (users): according to the Spanish Data Protection Agency's guidelines, information with regard to the processing of personal data (privacy policy) must be available both in the application itself and in the application store, so that the user can consult it before installing the application or at any time during its use. The language used in the privacy policies must be clear, taking into account the user target of the application. For example, applications available in Spanish and therefore aimed at Spanish-speaking users must provide the privacy policy in Spanish. In addition, the permissions that the application can request for access to data and resources should be indicated in the privacy policy.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

For example, it must explain if the application will process personal data only when it is being used by the user in the foreground or also when it is running in the background.

b) Privacy contractual considerations with data processors: the processing by the processor shall be governed by a binding contract that sets out the subject matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects and the obligations and rights of the controller. The contract must ensure that processing only takes place in accordance with the instructions of the data controller and prohibit the processor from reverting pseudonymised data in order to reveal the identity of the data subjects.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The main issue when sharing personal data in the context of digital health is that it is a market with many different players (app developers, device manufacturers, app stores, etc.). As the European Data Protection Supervisor established in its Opinion 1/2015 on Mobile Health, this makes it difficult to identify which parties act as data controllers or processors and to ensure an appropriate allocation of responsibilities, as well as ensuring user empowerment.

Therefore, it is important to respect the principle of transparency and accountability and the information requirements of Article 13 of the GDPR.

Moreover, in order to meet the obligations of privacy-by-design, it is important to clearly identify the different operators that will take part in the processing and to design the structure of all data processing activities accordingly. The above-mentioned Opinion states that data subjects should be given the option to freely allow the sharing/transfer of personal data to a third party, which is linked to the obligation of privacy-by-default, i.e. that the default features of the applications limit the types of processing to what is strictly necessary for the purposes of the application and/or device.

5.2 How do such considerations change depending on the nature of the entities involved?

Public authorities, unlike individuals, may transfer personal data concerning health without the consent of the data subjects, if it is necessary for the performance of a task carried out in the public interest or in the exercise of public authority and as long as it has a competence conferred by law.

According to the Spanish Data Protection Agency, if a certain processing is not "necessary" for the fulfilment of the mission carried out in the public interest or in the exercise of public powers conferred by law, such processing would lack a sufficient legal basis and would also infringe the principle of minimisation of data, which is also applicable to data processing carried out by public authorities.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Private entities may only share personal data if the data subject has provided their consent. There is also a legal obligation to transfer personal data that is essential for making decisions in public health to the health authorities.

Public authorities may transfer data subjects' health data without their consent to other public health authorities when this is strictly necessary for the protection of the population's health.

For purposes of biomedical research, it is necessary to collect the express written consent of the person concerned for the transfer of personal data to third parties not involved in medical care or biomedical research, even if the data is pseudonymised. In addition, if the data obtained from the source subject may reveal information of a personal nature about their relatives, the transfer to third parties shall require the express written consent of all the parties concerned.

6 Intellectual Property

6.1 What is the scope of patent protection?

The technologies involved in digital health may include medical devices, software and algorithms. Artificial intelligence and machine learning technologies are based on computational models and algorithms.

According to Article 4 of Law 24/2015 of 24 July 2015 on patents, computer programs, mathematical methods, plans, rules and methods for the pursuit of intellectual activities, for games or for economic and commercial activities and ways of presenting information, may not be patentable.

Therefore, the artificial intelligence and machine learning solutions *per se*, which are essentially software, i.e. a mathematical method, are not patentable. However, artificial intelligence-related inventions having a technical character would be patentable, since the patent would not relate to a mathematical method as such.

6.2 What is the scope of copyright protection?

According to the Spanish Copyright Act, the intellectual property of a literary, artistic or scientific work belongs to the author by the mere fact of its creation. Therefore, protection is granted without requiring the fulfilment of any kind of formalities, i.e. it is not necessary to register the work before any office. In Spain, the registration is merely for evidentiary purposes.

Copyright is the most common way to protect software. In this regard, Article 10(1)(i) of the Spanish Intellectual Property Act expressly foresees that computer programs are protected by copyright.

With regard to Artificial Intelligence solutions, which allow operators to process, analyse and extract useful information from huge data sets, according to Article 12 of the Spanish Copyright Act, these data sets could be copyright protected as data compilations.

6.3 What is the scope of trade secret protection?

Law 1/2019, of 20 February 2019 on Trade Secrets defines trade secrets as any information relating to any area of the company including technological, scientific, industrial, commercial, organisational or financial, which is secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question, its secrecy has commercial value and it has been subject to reasonable steps to keep it secret.

Trade secrets protection may be the only current existing option for protecting algorithms that are not be patentable.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

6.4 What are the typical results on academic technology transfer rules?

Results of academic technology are generally transferred to third parties through licence agreements, or as a result of the creation of a spin-off company.

Public research centres need to follow state regulations providing protection regarding the ownership of the creations, and are required to follow specific internal protocols that set out the terms for cooperation between university personnel and private entities.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Although the Spanish Patent Act expressly excludes the patentability of "computer programs", it seems to admit the possibility of patenting computer applications incorporated in patented hardware.

Another alternative to protect software would be through the Spanish Copyright Act, which expressly foresees the protection of computer programs. However, the protection granted by copyright is not as strong as patent protection, since the software will not be protected against the development of other programs meeting similar needs.

Other potential ways of protecting software are using trade secrets as well as trademarks legislation. However, regarding trade secrets, competitors may try to reverse engineer the software and it is key that reasonable steps are taken to keep it secret (such as signing non-disclosure agreements and prohibiting reverse engineering in licensing agreements).

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The Spanish Federation of Healthcare Technology Companies (FENIN) has a Code of Ethics which includes minimum principles to which its members must adhere when entering into collaboration agreements with healthcare professionals. The main requirements are that a legitimate need for the services must have been identified beforehand, that the agreements have to be documented in writing, all conditions should be agreed on market terms and be transparent, which means that the agreement should be notified in advance to the employer and that any publication or presentation of results will need to mention the collaboration.

Collaboration agreements should address confidentiality, ownership of the results, publication rights and adherence to ethical rules.

7.2 What considerations apply in agreements between health care and non-health care companies?

Any agreement with non-healthcare companies need to include an express commitment by the non-healthcare company to adhere to the ethical rules to which the health company adheres, in addition to the usual provisions regarding ownership of results, confidentiality and publication rights.

In the event that the digital health solution under development will need to be approved as a medical device, the agreement should address regulatory matters in order not to jeopardise approval.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning can be used for prediction of population health risks, enhancing health information management, quick and accurate diagnosis of conditions that are difficult to uncover or, for example, providing early health information to patients.

8.2 How is training data licensed?

Before licensing training data, it is vital to determine if healthcare data is involved, in which case the enhanced data protection principles apply. If anonymised, or at least pseudonymised, data can be used for the training purposes, these should be preferred.

Before licensing any data, the machine learning providers should obtain sufficient information about the provenance of the data, ascertain whether the data controller has collected the data in compliance with law, and whether they have sufficient permissions to apply the data in the training.

The agreement should further foresee the scope of permitted use of the licensed data and allocation of developed and derived data.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

The automatic learning algorithms learn from the information provided by their programmers and from there, they generate new works through a series of independent decisions, which may result in learning new methods or creation of new algorithms and models.

In Europe, the European Court of Justice has stated on several occasions, notably in its landmark Infopaq decision (case C-5/08, *Infopaq International A/S v. Danske Dagblades Forening*), that copyright only applies to original works and that originality must reflect the "author's own intellectual creation". This expression is generally understood to mean that an original work must reflect the author's personality. This can be interpreted to mean that there must be a human author for a copyright work to exist. In this case, it could be the programmer who owns the intellectual property rights.

If the machine learning process can be sufficiently described and put into use in a technical context, the subject matter could also fall within the patentable domain.

In this context, it is of vital importance that the parties involved in the machine learning process, generally at least the AI/machine learning provider and the provider of the data set used to teach the algorithm, must foresee beforehand in their contractual terms not only how the data input and resulting data can be used, but also how these data are going to be allocated and who will own the IP rights, such as trade secrets and patents, to the developed, clinical or derived data.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The foremost consideration in the licensing of data for their use in machine learning is the protection of personal data, due to the sensitivity of the data involved. The parties should address the provenance of the data and check that the necessary permissions to use such data are in place.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

The correct allocation of IP rights under licensing contracts is of the utmost importance in order to protect the parties and to secure the commercial viability of the project. Typically, it should be considered and foreseen beforehand who owns the background IP and the IP developed based (in part) on the other party's data, who owns and under what conditions the results and derived data may be used, and if there are any specific allocations, for example, for specific categories of data or assets.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Royal Legislative Decree 1/2007 of 16 November 2007, approving the revised text of the general law for the protection of consumers and users (GLPCU), imposes strict liability for personal injury or material damage that is caused by a defective product. The manufacturer of a product or an "own brander" (i.e. someone who, by putting their name, trademark or brand on a product, holds themselves out as the manufacturer) are primarily liable for defective products under the GLPCU.

The GLPCU will only apply to an algorithm or a solution if they are considered to be "products". In this regard, there are precedents of the Spanish High Court declaring that a software is considered a product.

This area is under review by the European Commission. An expert group established by the Commission has proposed changes to the liability regime in relation to AI, emerging digital technologies and the Internet of Things (Report on Liability for Artificial Intelligence and other emerging technologies issued by the Expert Group on Liability and New Technologies, dated 21 November 2019).

9.2 What cross-border considerations are there?

Suppliers (if they were aware of the defect) and importers of the defective product in the EU can also be liable. Liability is joint and several in the event that there are different potential liable parties.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Hospitals and healthcare professionals are increasingly relying on cloud-based services to store information related to patients and to make it accessible. Challenges in this area are the protection of personal data and prevention of cyber attacks.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Regulatory remains an important issue. Whether the digital health solution will require approval as a medical device has to be assessed from the outset through a risk classification of the product and this will affect the product development cycle. Non-healthcare companies will need to factor in longer product development cycles than for non-healthcare digital offerings.

Reimbursement strategies and developing a sustainable business model are becoming increasingly important. Non-healthcare companies need to understand the clinical problems they want to address and whether payers will see a value in it.

The healthcare provided in Spain is predominantly public. Therefore, the importance in gaining acceptance by public healthcare authorities also needs to be considered, in particular, whether the digital health solution satisfies an unmet and clearly identified need.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

The key issues are understanding the business model, clarifying the regulatory issues and the positioning of the product, and the specific revenue model, including potential reimbursement.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Montserrat Llopart has 30 years of experience advising on pharmaceutical and health law, compliance, contract law, licensing, competition law, regulatory changes and their implementation, M&A and general commercial matters.
She is the coordinator of the Compliance and Healthcare practice in the Baker McKenzie Barcelona Office and is a member of Baker McKenzie's EMEA Healthcare Steering Committee.
She advises companies in the healthcare sector regarding regulatory changes and their implementation and on financing and reimbursement issues. She also advises on the advertising and promotion of medicines and medical devices, including online advertising and social media.
Montserrat assists clients on a wide range of agreements related to the pharmaceutical industry, such as licence and distribution agreements, clinical trial agreements, and supply and manufacturing agreements.
She has considerable experience in the review of corporate compliance programmes, the drafting of codes of professional ethics and conducting compliance audits, and investigations.

Baker McKenzie
Av. Diagonal, 652
Edif. D, 8th Floor
Barcelona 08034
Spain

Tel: +34 93 206 0820
Email: montserrat.llopart@bakermckenzie.com
URL: www.bakermckenzie.com

Baker McKenzie is the first global law firm and operates from 78 offices in 46 countries around the world.
Baker McKenzie helps clients overcome the challenges of competing in the global economy. We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instil confidence in our clients.

www.bakermckenzie.com

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Sweden


Fredrika Allard


Annie Johansson


Johan Thörn

Advokatfirma DLA Piper KB

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no general definition of "digital health" in Swedish law. However, the Swedish Association of Local Authorities and Regions (SALAR) (Sw. *Sveriges Kommuner och Regioner*) has, together with other players such as the National Board of Welfare (Sw. *Socialstyrelsen*) and the eHealth Agency (Sw. *E-hälsomyndigheten*), defined "e-health" as the use of digital tools and digital exchange of information to achieve and maintain health. The definition of "health" is in turn based on the definition of health set by WHO, which is physical, psychological and social well-being.

1.2 What are the key emerging technologies in this area?

AI, VR-based technology, augmented reality, 3D-images and blockchain technology are technologies that have emerged in the area of healthcare IT.

According to a report issued by the National Board of Welfare (Sw. *Socialstyrelsen*) in October 2019, AI is however still in an early developmental stage within Swedish healthcare. Extensive research is being conducted but only a few applications are used in practice today. Politicians have proclaimed that Sweden will be leading in e-health by 2025. The aim is to increase digitalisation in healthcare, e.g. through use of e-prescriptions, mobile apps, online physicians and robots.

1.3 What are the core legal issues in health care IT?

Personal security and patient safety are core legal issues within healthcare IT. Confidence in digitalisation within the healthcare sector is largely affected by how well sensitive data is protected. Healthcare IT must also function so that it maintains the safety of the patients.

2 Regulatory

2.1 What are the core health care regulatory schemes?

- The Healthcare Act (SFS 2015:315).
- Patient Act (SFS 2014:821).
- Patient Injury Act (SFS 1996:799).
- Patient Safety Act (SFS 2010:659).
- Patient Data Act (SFS 2008:355).
- Patient Data Regulation (SFS 2008:360).
- The National Board of Health and Welfare's (Sw. *Socialstyrelsen*) regulations and general guidelines concerning patient records and processing of personal data within healthcare (HSLF-FS 2016:40).
- The National Board of Health and Welfare's (Sw. *Socialstyrelsen*) regulations and general guidelines concerning management system for systematic quality work (SOSFS 2011:9).
- The National Board of Health and Welfare's (Sw. *Socialstyrelsen*) regulation on the use of medical devices in healthcare (SOSFS 2008:1).

2.2 What other regulatory schemes apply to digital health and health care IT?

- The General Data Protection Regulation (EU 2016/679) (GDPR).
- The Swedish Act with supplementary provisions to the EU's Data Protection Regulation (SFS 2018:218).

2.3 What regulatory schemes apply to consumer devices in particular?

- The Product Safety Act (SFS 2004:451).
- The Product Liability Act (SFS 1992:18).
- Sales of devices to consumers are regulated by the Consumer Purchase Act (SFS 1990:932) and, in case of online sales, other e-commerce legislation such as the Distance and Doorstep Sales Act (2005:59).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

- The Medical Products Agency (Sw. *Läkemedelsverket*) (MPA) regulates and surveys the development, manufacturing and marketing of drugs and other medicinal products. Their task is to ensure that both the individual patient and healthcare professionals have access to safe and effective medicinal products and that these are used in a rational and cost-effective manner. The MPA also assumes the responsibility for market surveillance related to the law on medical devices and issuing directives with the support of this legislation.
- The Health and Social Care Inspectorate (Sw. *Inspektionen för Vård och Omsorg*, IVO) supervises health and social care, healthcare and social care staff, social services and activities in accordance with certain acts.
- The National Board of Health and Welfare (Sw. *Socialstyrelsen*) has duties and activities within the fields of social services, health and medical services, patient safety and epidemiology. The authority produces and develops standards, statistics, regulations and knowledge for the government and for those working in healthcare and social services. It also manages several different registers in the healthcare area.
- The Data Protection Authority (Sw. *Datainspektionen*) works to prevent encroachment upon privacy through information and by issuing directives and codes of statutes. The authority also handles complaints and carries out inspections.
- The Consumer Agency (Sw. *Konsumentverket*) safeguards consumer interests and is among other things the regulatory authority for the Product Safety Act. The Agency may require companies to comment on notifications against their goods and report on how they have ensured that the applicable security requirements are met. The Agency shares responsibility with other authorities that oversee specific goods or risks.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

- The Data Protection Authority (DPA) supervises how healthcare providers apply data protection regulations (GDPR and the Patient Data Act). The Patient Data Act contains provisions on the processing of personal data in healthcare. The DPA ensures that healthcare providers (both public and private) take security measures to protect patient data.
- There are a number of ongoing supervisory matters initiated by the DPA concerning access management to patient records. It is unclear when the DPA will issue its decisions.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Software which is classified as a medical device must comply with the Act on Medical Devices (1993:584). Depending on the type of device, specific regulations apply such as the Medical Products Agency's ordinance LVFS 2003:11 on medical devices, LVFS 2001:5 on active implantable medical devices and LVFS 2001:7 on *in vitro* diagnostic medical device.

The EU Medical Device Regulation 2017:745 (MDR) and the *In Vitro* Diagnostic Regulation 2017/746 (IVDR) regulations entered into force in May 2017. The regulations will become fully applicable following a transitional period of three years (MDR) and five years (IVDR) respectively. The MDR will become fully applicable as of 26 May 2020, while the IVDR will become fully applicable as of 26 May 2022. The new regulations replace the three current directives 90/385/EC on active implantable medical devices, 93/42/EC on medical devices and 98/79/EC on *in vitro* diagnostic medical devices. Some of the key changes are inclusion of products that were previously not covered by the directives' new classification rules and introduction of a unique device identification (UDI) system. The regulations also impose obligations on new actors such as distributors and importers.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Integrity and data security issues, e.g. hackers' intrusion in networks and theft of personal data.
- **Robotics**
  Difficulties in proving the cause of damages may result in difficulties to foresee liability under mandatory legislation.
- **Wearables**
  Integrity and data security issues, e.g. theft or loss of personal data, potentially sensitive personal data.
- **Virtual Assistants (e.g. Alexa)**
  See Telehealth.
- **Mobile Apps**
  See Wearables.
- **Software as a Medical Device**
  Under the MDR (see question 2.6) more stringent rules will apply to software classified as a medical device. Most medical device software is furthermore up-classified.
- **AI-as-a-Service**
  Security issues, e.g. data storage and access to data as well as data transit to servers, must be secured to ensure the data is not improperly accessed, shared or tampered with. The GDPR also prohibits transfer of data to countries outside the EU/EEA unless certain requirements are met.
- **IoT and Connected Devices**
  Integrity and data security issues, e.g. hackers' intrusion in networks in smart homes taking control of devices and theft of personal data. Data generated through use of IoT is almost always personal data, which means that specific rules apply, notably the GDPR.
- **Natural Language Processing**
  Training data may be limited as Swedish is a language which is spoken by a small population. Training data may be protected by copyright and/or contain personal data and may therefore not be used.

3.2 What are the key issues for digital platform providers?

Copyright may need to be addressed as well as GDPR issues. Dominant platforms need to comply with competition law. Platform providers of healthcare (e.g. hospitals, clinics) should also take into account the complexity of the healthcare legislation, such as the Patient Data Act (2008:355).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Use of personal data is governed by the General Data Protection Regulation (2016/679) (GDPR) and, depending on the situation, supplementary legislation, including the Data Protection Act (2018:18), the Patient Data Act (2008:355) and the Pharmacy Data Act (2009:367). Thus, it is important to establish if the use of personal data falls within the scope of these legal frameworks and observe the requirements laid down by the frameworks.

Key issues include: qualifying the role of the entities involved (i.e. whether the entity is a sole or joint data controller or a data processor); ensuring that the personal data is adequately protected (e.g. encryption and access management and logging); that the principles of personal data are observed; that there is a legal basis for the use of personal data (also special categories of personal data, e.g. health data); and that the data subjects (individuals) are duly informed of the use and third country (i.e. outside the EU/EEA) transfer restrictions.

4.2 How do such considerations change depending on the nature of the entities involved?

If more than one entity is involved in relation to a certain use of personal data (processing activity), each entity's role needs to be legally qualified, i.e. whether the entity is a sole or joint data controller or a data processor in relation to the use of personal data in a particular situation. It is important to determine which legal entity is the data controller in relation to *each* processing activity in data flow. One entity can have different roles in relation to different processing activities in the same data flow.

A data controller is defined under the GDPR as a "legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". The data controller is the entity mainly responsible for ensuring compliance. In principle, the entity exercising decisive control in relation to the use of personal data is deemed to be the data controller. The Patient Data Act and the Pharmacy Data Act provide that it is the healthcare provider and the authorised entity, respectively, that are the data controllers for the use of personal data that falls within the scope of respective legal framework.

A data processor is an entity that processes personal data on behalf of a data controller in accordance with the data controller's written instructions. The data processor has in certain situations a stand-alone obligation under the GDPR to ensure compliance with the legal framework (e.g. in relation to ensuring that the personal data is adequately protected).

4.3 Which key regulatory requirements apply?

The data controller must comply with certain key requirements, ensuring that:

(i) the use of personal data complies with the principles of processing personal data (including the principles of data minimisation, purpose limitation and storage limitation);
(ii) there is a legal basis for the processing of personal data (e.g. agreement, legal obligation, legitimate interest or consent);
(iii) there is an applicable exemption for the use of special categories of personal data (e.g. health data or biometric data), e.g. explicit consent;
(iv) the personal data is adequately protected (in this regard it shall be noted that the Swedish data protection authority requires that health data is encrypted in transit over open networks and that access over open network to health data is only granted to individuals whose identity is verified by way of strong authentication;
(v) the individuals are given information regarding the use of their personal data in accordance with the information and transparency requirements under the GDPR and potential supplementary legislation (e.g. the Patient Data Act);
(vi) there are data processing agreements in place with any data processors which use personal data on behalf of the data controller;
(vii) the restriction on third-country transfers are observed (please see below);
(viii) a prior data protection impact assessment (DPIA) is made before the use of personal data if the requirements for carrying out such a DPIA are triggered; and
(ix) the use of personal data is properly documented (e.g. covered by the data controller's records processing activities and that there are adequate documented routines and procedures in place to ensure and show compliance in practice).

In addition, as mentioned above, both the Patient Data Act and the Pharmacy Act include further requirements to be observed to the extent these legal frameworks apply (e.g. regarding use of personal data for certain defined purposes and security requirements such access management and encryption).

Moreover, if a public entity or organisation is involved, additional requirements may apply in relation to, e.g. disclosure and transfer of personal data under Public Access to Information and Secrecy Act (2009:400).

4.4 Do the regulations define the scope of data use?

The GDPR generally applies to use of personal data which is processed (wholly or partly) electronically and – in certain situations – also to personal data that is processed manually (physical form). Moreover, the principles of personal data (e.g. purpose limitation, data minimisation, etc.) under the GDPR limit the scope of data use. Moreover, to the extent special categories of personal data (e.g. health data) are processed, the data controller needs a specific exemption in order to process such personal data (e.g. explicit consent).

In addition, both the Patient Data Act and the Pharmacy Data Act further limits the use of personal data to specified purposes. Use of personal data outside these specified purposes require the individual's explicit consent.

4.5 What are the key contractual considerations?

To the extent a data processor is engaged in relation to the use of personal data, there must be a data processing agreement in place in relation to the data processor which needs to fulfil certain requirements laid down by the GDPR, e.g. that the data processor may only process personal data on documented instructions from the data controller and that the data processor shall take necessary measures to protect the personal data. The GDPR does not, however, govern commercial aspects of the relationship. As such, there is freedom to agree – between the parties – which measures the data processor shall be compensated for, but normally the data controller's starting point is that the data processor shall not be entitled to additional compensation (besides any service fee) for fulfilling obligations under law.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

In this regard, it is important to ensure that any service agreement and the data processing agreement is properly aligned.

Moreover, to the extent personal data is transferred outside the EU/EEA (third country), the parties may need to conclude a data transfer agreement which includes the EU Commission's standard contractual clauses for controller-to-controller or controller-to-processor transfers in order to ensure that the personal data is adequately protected.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The role of each entity involved must first be legally qualified in relation to *each* identified processing activity (use of personal data) in the same data flow in order to determine whether the entities are separate or joint data controllers or whether any entity is a data processor.

Where personal data is disclosed from one data controller (data exporter) to another data controller (data importer) for the data importer's own subsequent use of the personal data for its own purposes, the legal requirements under the GDPR (and potentially applicable supplementary legal frameworks) needs to be fulfilled both for the disclosure/transfer as such (data exporter is responsible) and for the subsequent use by the data importer (the data importer is responsible).

Please see above regarding use of data processors and the requirement to ensure that there is a data processing agreement in place.

Moreover, to the extent personal data is transferred outside the EU/EEA, the third country transfer restrictions under the GDPR must be observed. In principle, transfer of personal data outside the EU/EEA is restricted, unless an adequate level of protection can be ensured by way of appropriate safeguards or if a specific derogation from the restriction applies (e.g. explicit consent or the transfer is necessary for certain defined purposes such as the performance of a contract with the individual concerned). Appropriate safeguards include a data transfer agreement which includes the EU Commission's standard contractual clauses for controller-to-controller or controller-to-processor transfers.

5.2 How do such considerations change depending on the nature of the entities involved?

Please see responses above.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Since the sharing of personal data constitutes use (processing) of personal data as such, the same regulatory requirements apply as in relation to use of personal data – please see our comments above.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patents are protected under the Patents Act (SFS 1967:837). An application for a patent may be granted to any person who has made an invention which may have industrial application. A patent may only be granted for an invention which is new in relation to what was known prior to the date of the patent application and shall differ significantly therefrom.

Computer programs, mathematical methods and business methods are, however, exempt from the definition of an "innovation". An invention which has an industrial application which is, for example, effectuated by a computer program, may however be patentable.

The scope of patent protection is determined by the patent claims. A patent is granted for 20 years from date of application.

Inventions that arise as a result of an employee's activities or within the employment context are generally transferred to the employer under the Right to the Inventions of Employees Act (SFS 1949:345), provided that certain requirements are met. Teachers at universities, colleges or other institutions which are of an educational character, are not regarded as "employees" under the act.

6.2 What is the scope of copyright protection?

The Copyright Act (1960:729) protects literary and artistic works. Computer programs may be copyright protected, as well as preparatory design material for computer programs. In order to enjoy protection, the work must be original and be a manifestation of the author's creative efforts. Only works created by human beings are protected.

The scope of protection granted is, in principle, an exclusive right for the author to exploit the work by making copies of the work and making the work available to the public, in either the original or an altered form, via a translation or adaptation, in another literary or artistic form, or in another technical manner.

Copyright to a computer program which is created by an employee as part of his/her duties or following the instruction of the employer, is transferred to the employer, unless otherwise agreed.

Copyright protection arises automatically as soon as the work is created and is protected until the end of the 70th year after the year in which the author deceased. Copyright does not need to be registered in order to enjoy protection.

6.3 What is the scope of trade secret protection?

Trade secrets are protected by the Trade Secrets Act (2018:558). A trade secret is, in principle, defined as information concerning a company or its operations or a research institution's activities. The information must not be generally known or accessible to those who normally have access to information of the type in question. The information must further have been kept secret and the disclosure of the information must likely lead to competitive injury to the holder of the information.

The act contains provisions regarding damages, injunctions on pain of fine, and penalties for unauthorised misappropriation of trade secrets.

6.4 What are the typical results on academic technology transfer rules?

Teachers at universities, colleges or other institutions which are of an educational character are exempted from the definition of "employees" under the Right to the Inventions of Employees Act. Hence, they are also exempted from the general rule that the employer owns patentable inventions that arise as a result of an employee's activities or within the employment context ("the professor's privilege system"). The exclusive rights to patentable

© Published and reproduced with kind permission by Global Legal Group Ltd, London

inventions remain with the inventor, leaving him/her the right to, for example, commercialise the rights, unless otherwise agreed.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Software as a medical device may be protected by copyright laws, *cf.* question 6.2.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The Swedish Association of Local Authorities and Regions (Sw. *Sveriges Kommuner och Regioner, SKR*) (SALAR) and the industry associations for the pharmaceutical industry (LIF), the medical device industry (Swedish Medtech), and the laboratory industry (Swedish Labtech) have agreed on common rules for collaborations and interactions between the industry and healthcare. The agreement includes rules on collaborative improvements between the parties, referred to as "development projects". The rules shall be applied by SALAR also in relation to companies which are not part of the industry associations but which are active within the relevant fields.

The basic principles for all collaborations are documentation, transparency and reasonability, in addition to the collaboration being to the benefit of all parties. An agreement regarding a development project must be made with a healthcare unit/department; not with an individual employee. All parties must contribute to the project with time, material and financial means. The contributions must be balanced between the parties. Healthcare must always bear its own administrative costs connected with the project. The project must furthermore be limited in time (maximum one year). A detailed project plan must be available, regulating e.g. how the project shall be evaluated as well as a budget. The project must furthermore be transparent and disclosure of transfers of value may be required if a pharmaceutical company is involved.

7.2 What considerations apply in agreements between health care and non-health care companies?

The agreement should reflect the ethical rules and principles of best practice that the healthcare industry and the other industry have set up (*cf.* question 7.1).

The agreement should describe the roles and contributions of each party, as well as regulate rights to intellectual property, confidentiality issues and compliance with other legislation and regulations, etc.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning is primarily used in taking medical history and patient contacts. It is also said to increase in the areas of diagnosis and decision support.

8.2 How is training data licensed?

There is no typical mode of licensing training data.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

The Copyright Act provides protection for works which are created by human beings. Whether works created by autonomous AI can be regarded as "works" under the act is debated. Further, the work must be created by a human being in order to enjoy protection. Since the creator of the AI cannot predict or affect what the AI will create, the results will not be a manifestation of human creativity and the results are therefore probably not protected by Swedish copyright laws. Ownership to data should instead be regulated by way of agreements.

8.4 What commercial considerations apply to licensing data for use in machine learning?

How and for which purposes the data may be used should be regulated in the license agreement as well as ownership of data. If the data contains personal data, data security issues (including the GDPR) may need to be addressed, which will also be the case if the data is commercially sensitive data. Other factors that may need to be regulated are confidentiality, rights to sublicense the data, as well as ethical considerations.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Under the Patient Injury Act (SFS 1996:799) healthcare providers (both private and public) must have patient insurance that covers compensation for personal injuries that have arisen in connection with healthcare in Sweden. The right to compensation from the patient insurance arises when there is either a direct link to a treatment of the patient or if the injury has been caused by a defect in a medical device or other pharmaceutical equipment, or if it is a result of an error or neglect by a healthcare professional according to the detailed criteria set out in the Act.

The Product Liability Act (SFS 1992:18) is a liability law that imposes a strict liability on manufacturers and importers for personal injury (on any person) or property damage to consumers' property, caused by a safety deficiency in products. By "products" movable property is meant. A product has a safety deficiency if it is not as secure as can be expected.

The Liability Act (SFS 1972:207) regulates non-contractual liability, i.e. when damage has occurred unrelated to a breach of a contract. A person who wilfully or negligently causes a personal or property injury shall compensate the damage. Economic loss which has arisen unrelated to a personal or property injury is compensated if it was caused either by a criminal act or as a result of incorrect information or advice from an authority through error or neglect.

9.2 What cross-border considerations are there?

The Product Liability Act, which implements the Product Liability Directive (85/374/EEC), imposes a joint responsibility on the importer and the manufacturer in cases where the product is imported from a non-EU country for sales within the EU.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

10 General

10.1 What are the key issues in Cloud-based services for digital health?

eSam, a member-driven program for collaboration between authorities and the Swedish Association of Local Authorities and Regions (SALAR), has issued a statement regarding cloud-based services used by public entities and organisations. In short, eSam considers that it cannot be ruled out that a cloud service provider, which is subject to foreign legislation, can contribute to the disclosure of information which is subject to secrecy under the Public Access to Information and Secrecy Act (2009:400). It is said that the statement prohibits use of, e.g. cloud-based services where the server is placed in the U.S. A triggering factor behind the statement is the U.S. legislation, the Cloud Act.

Please also see sections 4 and 5 regarding transfer of personal data outside the EU/EEA.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Sweden is a tech-savvy nation with the majority of the population having access to Internet. With the government's goal to be the best in the world in e-health by 2025, along with an ageing population which poses financial challenges and resource constraints in public healthcare, which in Sweden is provided to all citizens, Sweden provides a good market for digital solutions. However, bureaucracy, complex organisations, and remuneration systems that can provide the wrong incentives may constitute obstacles. The complexity of the laws regulating Swedish healthcare should furthermore not be underestimated.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

Implementing the right incentives in order to ensure that management remains with the company after take over in order to not lose valuable knowledge and expertise.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Fredrika Allard has worked within the Life Sciences sector for the past decade and heads the Life Sciences group within DLA Piper Sweden. She also forms part of the firm's Intellectual Property and Technology group.
Fredrika primarily works with regulatory issues in the pharmaceutical and medical device sectors. Her practice encompasses, among other things, legal issues relating to clinical trials, biobanks and drafting various types of agreements relevant in the sector. She also has extensive experience in the marketing of pharmaceuticals and the rules regulating the co-operation between the pharmaceutical industry and healthcare personnel. Fredrika has for several years held the position as secretary of the Information Practices Committee (the NBL) and is a recurrent speaker at the course for information officers in marketing ethics, which is provided on behalf of the trade association LIF.
Fredrika also works with different types of IT and commercial agreements, consultancy and cooperation agreements in various sectors.

Advokatfirma DLA Piper KB
Kungsgatan 9
103 90 Stockholm
Sweden

Tel: +46 8 701 78 00
Email: fredrika.allard@dlapiper.com
URL: www.dlapiper.se

Annie Johansson has worked in DLA Piper's Life Science group for more than 10 years, specialising in marketing and other regulatory issues within the pharmaceutical industry. She has also worked with regulatory issues within the medical device sector. She has, between the year 2009 and 2019, had the role as secretary for the Information Practices Committee (NBL), the self-regulatory system within the pharmaceutical industry in Sweden. Annie also regularly lectures on the ethical rules of the pharmaceutical industry.

Advokatfirma DLA Piper KB
Kungsgatan 9
103 90 Stockholm
Sweden

Tel: +46 8 701 78 00
Email: annie.johansson@dlapiper.com
URL: www.dlapiper.se

Johan Thörn is a senior associate in the firm's Employment, Data Protection and Life Sciences groups.
He has substantial experience advising clients on a various data privacy issues, including screening against sanction lists, customer profiling, drafting of data processing agreements, cookies compliance, e-signature advice, cross-border and global data transfers (including the local adoption of Binding Corporate Rules). He has extensive expertise in GAP analysis, data protection impact assessments and mapping of all data processing activities in this regard in order to ensure compliance with data privacy laws, including the General Data Protection Regulation (GDPR). Furthermore, he regularly assists with data breaches handling from a GDPR perspective.

Advokatfirma DLA Piper KB
Kungsgatan 9
103 90 Stockholm
Sweden

Tel: +46 8 701 78 00
Email: johan.thorn@dlapiper.com
URL: www.dlapiper.se

DLA Piper is the leading global business law firm in Sweden. The Stockholm office employs 160 people, of which over 110 are lawyers. The firm provides legal advice in all areas of business law, which includes: corporate; banking and finance; IT; media; intellectual property; tax; M&A; capital markets; transport and logistics; private equity; litigation; insurance; regulatory; insolvency; and employment.
The firm has a large and growing Swedish and international client base consisting of companies, government agencies and organisations with a wide variety of business activities such as industry, manufacturing, services, real estate, banks and financial companies, IT and telecommunications, media, etc.
DLA Piper is a global law firm with offices in more than 40 countries, positioning us to help companies with their legal needs anywhere in the world.

We provide clients with trusted local expertise and access to seamless multi-jurisdictional legal capabilities across a range of services and sectors.
www.dlapiper.se

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Switzerland

Dr. Stefan Kohler

Christian Wyss

VISCHER

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

In Switzerland, digital health is not a legal term. In general, the term covers services and equipment that use information and communication technologies (ICT) in healthcare to improve healthcare and public health. In agreement with this, the Swiss government defines the term "eHealth" as the integrated use of ICT to design, support and network all processes and participants in the healthcare system.

1.2 What are the key emerging technologies in this area?

Numerous digital health solutions are currently being tested and implemented. The following solutions could become relevant in the coming years and possibly lead to disruptive innovations:

- Wearables: Mobile sensors that are worn directly on the body which continuously collect physiological data (e.g. blood pressure, temperature, pulse) and evaluate them in real time.
- Health monitoring and care using robots and sensors: Robots and/or room sensors are used to monitor and care for patients or other people in need of care (e.g. in nursing homes).
- Digital avatars and assistance systems: Computer-supported artificial and graphic representations of a person, which support people visually and/or linguistically in a task (e.g. virtual school lessons for children in hospital).
- Machine learning and predictive analysis: Based on artificial intelligence (AI), software systems process and analyse large amounts of data and automatically optimise themselves (e.g. efficient analysis of DNA sequences with AI-based mechanisms for the detection of genetic diseases).
- Online health counselling: Health-related counselling services, diagnoses and referral to doctors can be obtained on digital platforms or apps (e.g. dermatological diagnoses or health insurance counselling services).

1.3 What are the core legal issues in health care IT?

According to Swiss law, personal health data are considered "particularly worthy of protection". Accordingly, data security and data protection are regularly the main issue with digital health solutions. Providers of digital health solutions, such as wearables, health apps or electronic patient records (EPR), must comply with the applicable data protection regulations, in particular the Federal Data Protection Act and – in the European context – the General Data Protection Ordinance (GDPR). In addition, other decrees may be relevant in Switzerland, such as the Federal Law on Human Genetic Testing or the Human Research Act.

Further legal issues:

- The cantons sometimes set different standards in the field of digital health, which can make it difficult to introduce digital health applications uniformly throughout Switzerland. However, for providers of digital healthcare solutions, the differences between the cantons can also provide scope for implementing an innovative business idea.
- In the field of telemedicine and other digital service areas, the billing and remuneration models are still largely unclear. The currently applicable tariff system covers digital services incompletely. Incentives for digital health solutions are missing.
- There are still uncertainties regarding the qualification of software and apps as medical devices and the conformity assessment of such solutions.

2 Regulatory

2.1 What are the core health care regulatory schemes?

- **Therapeutic Products**
  - Federal Act on Medicinal Products and Medical Devices (Therapeutic Products Act, TPA; no. 812.21).
  - Ordinance on Licensing in the Medicinal Products Sector (no. 812.212.1).
  - Ordinance on Medicinal Products (no. 812.212.21).
  - Ordinance on the Advertising of Medicinal Products (no. 812.212.5).
  - Medical Devices Ordinance (MedDO; no. 812.213).
  - Ordinance on the List of Medical Devices Subject to Prescription (no. 812.213.6).
  - Ordinance on Integrity and Transparency in the Therapeutic Products Sector (no. 812.214.31).
- **Research on Humans**
  - Federal Act on Research involving Human Beings (Human Research Act, HRA; no. 810.30).
  - Ordinance on Human Research with the Exception of Clinical Trials (Human Research Ordinance, HRO; no. 810.301).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- Ordinance on Clinical Trials in Human Research (Clinical Trials Ordinance; ClinO; no. 810.305).
- Ordinance on Organisational Aspects of the Human Research Act (HRA Organisation Ordinance, OrgO-HRA; no. 810.308).
- Federal Act on Research Involving Embryonic Stem Cells (Stem Cell Research Act, StRA; no. 810.31).
- Ordinance on Research involving Embryonic Stem Cells (Stem Cell Research Ordinance, SCRO; no. 810.311).

- **Transplantation**
  - Federal Act on the Transplantation of Organs, Tissues and Cells (Transplantation Act; no. 810.21).
  - Ordinance on the Transplantation of Human Organs, Tissues and Cells (Transplant Ordinance; no. 810.211).
  - Ordinance on the National Cross-Over Living Donation Programme (no. 810.212.3).
  - Ordinance on the Allocation of Organs for Transplantation (no. 810.212.4).
- **Communicable Diseases**
  - Federal Act on Protection against Infectious Diseases in Humans (Epidemics Act, EpidA; no. 818.101).
  - Ordinance on Protection against Infectious Diseases in Humans (no. 818.101.1).
- **Medically Assisted Reproduction and Genetic Testing**
  - Federal Act on Medically Assisted Reproduction (Reproductive Medicine Act; no. 810.11).
  - Reproductive Medicine Ordinance (no. 810.112.2).
  - Ordinance on the National Ethics Committee in the Field of Human Medicine (no. 810.113).
  - Federal Act on Genetic Testing of Human Beings (no. 810.12).
  - Ordinance on Genetic Testing of Humans (no. 810.122.1).
  - Ordinance on the preparation of DNA Profiles in Civil and Administrative Matters (no. 810.122.2).
- **Requirements for Healthcare Professionals**
  - Federal law on the University Medical Professions (Medical Profession Act, MedBG; no. 811.11).
  - Medical Profession Ordinance (no. 811.112.0).
  - Cantonal implementing legislation on healthcare professionals.
- **Health Insurance and Reimbursement**
  - Federal Act on Health Insurance (HIA; no. 832.10).
  - Ordinance on Health Insurance (HIO; no. 832.102).
  - Ordinance on Benefits in the Compulsory Health Insurance (HIBO; no. 832.112.31).
  - Ordinance on the Determination of Costs and the Recording of Services by Hospitals, Birth Centres and Nursing Homes in Health Insurance (no. 832.104).

2.2 What other regulatory schemes apply to digital health and health care IT?

- **Data Protection**
  - Federal Act on Data Protection (FADP, no. 235.1).
  - Ordinance to the Federal Act on Data Protection (no. 235.11).
- **Electronic Patient Record (EPR)**
  - Federal Act on the Electronic Patient Record (EPRA; no. 816.1).
  - Ordinance on the Electronic Patient Record (no. 816.11).
  - Federal Council Ordinance on the Electronic Patient Record (no. 816.111).
  - Federal Council Ordinance on Financial Aid for the Electronic Patient Record (no. 816.12).
  - Departmental Ordinance on the Electronic Patient Record.
  - Cantonal legislation: Cantons must check their respective legal systems for compatibility with the EPRA and its implementing law and, if necessary, initiate adjustments.

2.3 What regulatory schemes apply to consumer devices in particular?

So far, there are no special legal regulatory schemes for digital health devices in Switzerland. With regard to the warranted properties and the rights of consumers in relation to defects, the rules of contract law in the Swiss Code of Obligations (no. 220) apply. The Federal Act on Product Liability (no. 221.112.944) may (additionally) be relevant for liability in cases of personal injury, and the Federal Act on Product Safety (no. 930.11) for product safety requirements.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

- **Swiss Agency for Therapeutic Products (Swissmedic)**
  Swissmedic (with headquarters in Berne) is responsible for the enforcement of the Swiss legislation on therapeutic products. Swissmedic's remit mainly involves the granting of marketing authorisations and operating licences and market surveillance. Swissmedic's enforcement competence also includes the ordering of administrative measures and/or administrative criminal investigations.
- **Federal Office of Public Health (FOPH)**
  The FOPH is generally responsible for the health of the Swiss population, develops Swiss health policy and is committed to a health system that is efficient and affordable in the long term. Among other things, the FOPH deals with questions concerning reimbursement of medical analysis and treatments, pharmaceuticals and medical devices by health insurers. The FOPH is also responsible for the enforcement of the integrity and transparency regulations in the field of therapeutic products. The FOPH's enforcement competence also includes the ordering of administrative measures or administrative criminal investigations.
- **Cantonal Authorities**
  Cantonal Authorities are responsible for the surveillance and enforcement of the Swiss legislation on therapeutic products in specific areas (e.g. carrying out inspections and quality controls). In the course of their monitoring services, the cantons shall notify Swissmedic or the FOPH in accordance with their respective responsibilities of any events, findings or complaints.
  Cantons issue the authorisation of mail-order trade in the health sector.
- **eHealth Suisse**
  To implement the eHealth strategy in Switzerland, the Federal Department of Home Affairs (FDHA) and the Conference of Cantonal Health Directors (CDC) jointly run the eHealth Suisse competence and coordination centre. The aim of eHealth Suisse is to define common organisational, legal and technical guidelines for the development of eHealth applications, in particular the EPR.
  eHealth Suisse has no enforcement competence as such.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

- Enforcement of notification, authorisation and/or certification obligations (e.g. for applications qualifying as medical devices; for online medical consultation).
- Enforcement of data security and data protection obligations.
- Enforcement of restrictions applicable in the field of online genetic analyses, online diagnostic tests or other online medical services.
- Enforcement of restrictions in the area of pharmaceuticals (e.g. advertising restrictions, prescription restrictions, integrity obligations).
- Enforcement of professional obligations that medical personnel must comply with.
- Enforcement of the conditions that apply to reimbursement of digital health services by health insurance companies.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

For medical devices, including digital health solutions, the following legislation on therapeutic products is primarily relevant:

- Therapeutic Products Act (TPA; no. 812.21).
- Ordinance on Medicinal Products (no. 812.212.21).

For the practical implementation of the legislation on therapeutic products, with particular reference to software-based medical devices, the competent Swiss authorities have published the following guidelines (as amended from time to time):

- Swissmedic Leaflet on Standalone Medical Device Software [AW-Merkblatt Eigenständige Medizinprodukte-Software].
- eHealth Suisse: Guide for App Developers, Manufacturers and Marketers.

Switzerland has concluded agreements on the mutual recognition of conformity assessments for medical devices (bilateral agreements or mutual recognition agreements – MRAs) with the EU Member States, the EFTA States and Turkey. The basis of these agreements is the application of the European directives for medical devices and the European CE marking. The countries concerned recognise the certificates issued by Swiss conformity assessment bodies and, in return, Switzerland recognises the conformity assessments carried out by Notified Bodies/Conformity Assessment Bodies in the countries concerned.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  - Depending on their characteristics, telehealth platforms may qualify as medical devices. If so, the compliance of the platform with the legal requirements needs to be assessed by a Conformity Assessment Body (CAB).
  - Telehealth platforms as such may be subject to a notification or licensing requirement. The cantonal implementing legislation, including that on healthcare professionals, must be observed. It should be noted that the cantonal regulations in this regard are not uniform.
  - The health data transferred via telehealth platforms are considered to be particularly worthy of protection. The platform operator must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - There are certain limits to diagnosis and treatment via telehealth platforms. Medical due diligence must be ensured at all times. According to the case law of the Swiss Federal Supreme Court, prescribing medicines via telehealth platforms requires that the patient receives personal and serious advice from a doctor.
  - The responsibility and liability between the operators of the platform and the involved healthcare professionals must be clearly regulated both in the internal relationship (operator-doctor) and external relationship (operator-customers; doctors-patients).
- **Robotics**
  - Depending on their characteristics, robotic technologies used in healthcare may qualify as medical devices. If so, the compliance of the robot with the legal requirements needs to be assessed by a CAB.
  - If the robot is capable of collecting personal data, the operator must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the robot provides users with instructions or recommendations on certain behaviour. The allocation of liability issues between the parties involved (e.g. manufacturer, healthcare institution, health care professionals) must be contractually regulated.
  - The use of robots, especially in elderly and patient care, can affect the personal rights of those in need of care. Prior informed consent of the persons in need of care (or their legal representatives) should therefore be obtained.
- **Wearables**
  - Depending on their characteristics, wearables may qualify as medical devices. If so, the compliance of the device with the legal requirements needs to be assessed by a CAB.
  - Wearables collect and evaluate health data. The manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the wearables provide users with instructions or recommendations on certain behaviour.
- **Virtual Assistants (e.g. Alexa)**
  - Virtual assistants collect and evaluate personal data, including health data. The manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the virtual assistants provide users with instructions or recommendations on certain behaviour.
  - Virtual assistants can affect the personal rights of users. Prior informed consent of the users (or their legal representatives) should therefore be obtained.
- **Mobile Apps**
  - Depending on their characteristics, mobile apps may qualify as medical devices. If so, the compliance of the mobile app with the legal requirements needs to be assessed by a CAB.
  - If the mobile app is capable of collecting personal data, the manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the mobile app provides users with instructions or

© Published and reproduced with kind permission by Global Legal Group Ltd, London

recommendations on certain behaviour. The allocation of liability issues between the parties involved (e.g. manufacturer, operator, health insurance company, healthcare professionals) must be contractually regulated.

- **Software as a Medical Device**
  - Compliance of the device with the medical device regulations needs to be assessed by a CAB.
  - The manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the device provides users with instructions or recommendations on certain behaviour. The allocation of liability issues between the parties involved (e.g. manufacturer, operator, health insurance company, healthcare professionals) must be contractually regulated.
- **AI-as-a-Service**
  - Depending on its characteristics, AI-as-a-service may qualify as a medical device. If so, the compliance of the service with the legal requirements needs to be assessed by a CAB.
  - Given the large amounts of data from a variety of sources used in AI systems, AI systems are prone to errors. The establishment and maintenance of a continuous and effective quality assurance concept is indispensable. The liability issues associated with AI in healthcare need to be carefully contractually allocated between the parties involved (e.g. manufacturer, operator, health insurance company, healthcare professionals).
  - AI systems requires large amounts of data from sources such as electronic health records, pharmacy records, insurance claims records, or patient-generated information. The operators of AI systems must ensure compliance with data protection legislation (including that on cybersecurity).
- **IoT and Connected Devices**
  - If the IoT and/or connected devices are capable of collecting personal data, the manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the IoT and/or connected devices provide users with instructions or recommendations on certain behaviour. The allocation of liability issues between the parties involved (e.g. manufacturers, operators, etc.) should be as far as possible contractually regulated.
- **Natural Language Processing**
  - Natural language processing involves the processing and analysis of large amounts of natural language data. If these data can be attributed to a specific person (i.e. are not anonymised), the data protection legislation is relevant.

3.2 What are the key issues for digital platform providers?

The key legal issue with digital platforms is the question of whether the platform provider or the user (uploader) is responsible and liable for the uploaded content. There is no specific legal basis on this issue in Switzerland. Relevant in this regard are, on the one hand, the provisions of the Federal Law against Unfair Competition (no. 241) and, on the other hand – if statements that violate personality rights are in question – the civil and criminal law provisions on the protection of personality rights (in particular Art. 28 of the Swiss Civil Code: no. 210). According to Swiss legal practice, it is undisputed that the uploader is responsible for the uploaded content. Under certain circumstances, however, the platform provider may be held responsible for the content of the platform users as well. Accordingly, the Swiss Federal Supreme Court confirmed in its (attorney-criticised) decision no. 5A_792/2011 the joint responsibility of the provider in the case of a violation of personality rights committed via the platform (Art. 28 ZGB). Digital platform providers must therefore be aware that they do not have a general liability privilege in Switzerland for user content on the platform. Platform providers should exclude the respective liability risk as far as possible with suitable contractual agreements.

Another important issue is data protection and data security. Platform providers are required to implement the relevant requirements of data protection legislation on their platform.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Data that is truly anonymised does not fall under data protection laws. As a result, it can be freely used for any purpose, including medical research. However, when large amounts of data are analysed, anonymisation reaches its limits. The comparison of anonymised data with other data entails the risk of reidentification of the previously anonymised data. Health data in particular is highly individualised, which makes effective anonymisation difficult. Using personal data for digital health applications means that all requirements of the applicable data protection laws must be complied with.

4.2 How do such considerations change depending on the nature of the entities involved?

Swiss data protection law is technology-neutral. Note that all listed hospitals execute cantonal performance mandates and thus fall within the scope of cantonal data protection laws. Not only public listed hospitals but also private listed hospitals have to comply with cantonal data protection law unless there is special legislation that provides for an exemption. For hospitals without cantonal performance mandates and for all private digital health providers, the Swiss Federal Data Protection Act applies.

In addition, the GDPR also applies to Swiss digital health providers offering their services in EU countries.

4.3 Which key regulatory requirements apply?

The processing of data relating to specific or identifiable persons is subject to the Data Protection Act and under certain circumstances to the GDPR. In contrast to European law, Swiss law does not prohibit processing subject to permission as long as the processing is carried out lawfully and in accordance with the data processing principles of Art. 4, 5 and 7 FADP (*cf.* Art. 12 para. 2 lit. a FADP). These are:

- Principle of transparency: The collection of personal data and in particular the purpose of their processing must be identifiable to the data subject (Art. 4 para. 4 FADP).
- Principle of purpose limitation: Personal data may only be processed for the purpose that was stated at the time

© Published and reproduced with kind permission by Global Legal Group Ltd, London

of acquisition, is apparent from the circumstances or is provided for by law (Art. 4 para. 3 FADP). As soon as the data processing goes beyond the purpose, justification, a legal basis or consent is necessary.

- Principle of proportionality: The processing of personal data must be proportionate, i.e. must not go further than the purpose of the processing requires (Art. 4 para. 2 FADP).
- Principle of data integrity: The processor must ensure the accuracy of the personal data and destroy incomplete or inaccurate personal data (Art. 5 para. 1 FADP).
- Principle of data security: Personal data must be protected against unauthorised processing by appropriate technical and organisational measures (Art. 7 para. 1 FADP).

Consequently, Swiss law does not require the consent of the person concerned or any other justification for the lawfulness of the processing of health data. It is sufficient for the person concerned to be informed of the purpose of the processing and the processor to comply with the purpose limitation principle and the other processing principles.

As already mentioned above, the GDPR has extraterritorial effects; therefore Swiss service providers may also be affected.

The GDPR contains stricter regulations than the current FADP. Thus, the principle of prohibition subject to permission applies here. Permission can arise from the law or from the consent of the person concerned. However, the total revision of the FADP, where the draft is currently being discussed in parliament, will bring it into line with the GDPR. For example, according to the new draft, data managers and processors will have to take appropriate measures to reduce the risk of personal injury as early as the planning stage of data processing. In addition, they are obliged to ensure, by means of appropriate default settings, that only personal data that is relevant for the respective purpose is used (such as pseudonymisation, where knowledge of the data subject is not necessary for the processing). The new E-FADP is expected to enter into force in 2021.

With regard to medical research, further provisions of the Human Research Act must be observed. The Human Research Act allows the anonymisation of data and their subsequent use for research on humans only if it is not biological material or genetic personal data, or if the person concerned has been informed in advance and has not submitted his or her veto (Art. 32 para. 3 HRA).

Furthermore, a recent judgment in which the Federal Administrative Court had to assess the procurement of data by the supplementary health insurance provider from the compulsory health insurance within the same group showed that, in addition to the FADP, the data transfer provisions of Art. 84a of the Federal Health Insurance Act are also highly relevant for digital health providers.

4.4 Do the regulations define the scope of data use?

On the basis of the principle of proportionality pursuant to Art. 4 para. 2 FADP, the processing of data may not go beyond what is necessary for the purpose of processing. Accordingly, no data may be collected in stock.

4.5 What are the key contractual considerations?

Art. 4 para. 4 FADP provides that the data collection and the purpose of the processing must be identifiable for the data subject. According to Art. 4 para. 3 FADP, the processing of personal data may only be carried out for the purpose stated at the time of collection, which is apparent from the circumstances or is provided by law. Explicit consent is required for the collection of particularly sensitive personal data, such as data on health. However, such consent is only valid if the person has been adequately informed and has subsequently given his or her informed consent voluntarily. In addition, the consent can also be withdrawn at any time, whereby the burden of proof for the existence of the consent lies with the data processor in each case. For the information to be considered appropriate to the data subject, it must at least cover the type, scope and purpose of the data processing, the names of the data processors and, if applicable, the risks of the data processing (informed consent). Due to these requirements regarding the adequacy of information, blank consent to any future form of processing is only possible if it is carried out with clear limits. In principle, it is also possible to integrate data protection provisions into general terms and conditions if the data subjects are adequately informed about the scope of their consent and the data protection provisions are presented clearly enough. Here too, however, explicit consent is required for data on health. In addition, Art. 8 of the Federal Act Against Unfair Competition prohibits general terms and conditions that, against the principles of good faith, provide for a significant and unjustified disproportion between a consumer's contractual rights and obligations to the detriment of the consumer. Data subjects of health data qualify as consumers. Thus, general terms and conditions must not only ensure that the data subjects explicitly consent to having their health data processed, but must also provide for a reasonable balance of the data subject's contractual rights and obligations.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Art. 10a FADP allows the use of data processors unless prohibited by legal or contractual confidentiality obligations. The data subject must be informed, however, in the case of a transfer of the personal data to a country that does not have an adequate level of data protection.

5.2 How do such considerations change depending on the nature of the entities involved?

The duty to provide information and the right of access to personal data may vary depending on whether the personal data were obtained from the data subject themselves or not. If the personal data have not been obtained from the data subject, the responsible person must also provide the contact details of the data protection officer and the categories of personal data processed. In addition, the data subject must be provided with information on the source of the data and whether these sources are publicly available.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The disclosure of particularly sensitive data (health data) to third parties always requires justification (Art. 12 para. 2 lit. c FADP). If the justification lies in the consent of the data subject (Art. 13 para. 1 FADP), this must be given voluntarily and explicitly after appropriate information (Art. 4 para. 5 FADP). The data subject then always has the opportunity to object to the processing (Art. 12 para. 2 lit. b FADP).

According to the new draft of the FADP, the list will extend the existing list of particularly sensitive personal data. Genetic

© Published and reproduced with kind permission by Global Legal Group Ltd, London

and biometric data (e.g. fingerprints), which uniquely identify a natural person, have recently also been taken into account.

6 Intellectual Property

6.1 What is the scope of patent protection?

Inventions are subject to patent protection, i.e. new technical solutions to technical problems, whereas private use, research and teaching are excluded from the protective effect of a patent. What is unique to Switzerland is that there is no official examination for novelty or an inventive step. The scope of protection is defined in the patent claims and the period of protection is a maximum of 20 years, whereby a Swiss patent automatically also applies in Liechtenstein. Switzerland is a member of all major regional and international patent treaties, including the European Patent Convention (EPC) and the Patent Cooperation Treaty (PCT).

6.2 What is the scope of copyright protection?

Literary and artistic intellectual creations (including computer programs) with an individual character are subject to copyright protection, irrespective of their value or purpose. Such creations automatically become protected at the moment of creation. The author has the exclusive right to his own work and the right to recognition of his authorship. The author has the exclusive right to decide whether, when, how and under what author's designation his own work is published for the first time. The period of protection is up to 70 years after the death of the author (50 years for computer programs). What is unique to Switzerland are the collective rights management organisations such as SUISSIMAGE. Moreover, various international agreements on copyright, such as the Revise Berne Convention (WCT), ensure that Swiss authors receive the same protection as foreign authors.

6.3 What is the scope of trade secret protection?

Though Switzerland lacks specific trade secret laws, many aspects of trade secret protection are adequately covered. For instance, there are provisions on certain aspects of trade secrets protection in the Unfair Competition Act (no. 241; e.g. prohibition of exploitation or use of trade secrets that were unlawfully obtained), the Criminal Code (i.e. anyone who divulges a trade secret that he is under a statutory or contractual duty not to reveal, or anyone who exploits for himself or another such a betrayal, is liable to criminal sanctions), and the Code of Obligations (i.e. employment law: employees must not exploit or reveal confidential information – such as trade secrets – obtained while in the employer's service). As a consequence of the diversity of legal provisions on trade secrets, there is no unique protection theory on trade secrets in Switzerland.

6.4 What are the typical results on academic technology transfer rules?

Most public research and educational institutions and university hospitals (PROs) in Switzerland have professionally organised bodies that ensure technology transfer with the private sector. Uniform regulations on this technology transfer are drawn up by the Swiss Technology Transfer Association (swiTT). The following main principles apply:

- Partnership: The cooperation between private enterprise and PROs rests on the basis of partnership. PROs are entitled to an appropriate financial share of the revenues generated by the cooperation partner through commercialisation of the intellectual property rights.
- Intellectual Property: As a rule, the PROs claim the intellectual property rights created by them within the scope of the cooperation for themselves, but grant the industrial partner exclusive rights of use.
- Freedom of Publication: The publication of scientifically interesting research results remains a central task of PROs. Before publication, adequate time for the preparation and submission of a patent application is contractually provided.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Under the prevailing Swiss doctrine, the term "software" is a generic term comprising both the computer program and the development and user documentation. Accordingly, for software as a medical device, copyright protection is paramount. Copyright law thus protects the concrete implementation, i.e. the program code, but not a process underlying a computer program.

The software used in a medical device as such cannot be protected by patents. However, computer programs used to implement a technical invention, so-called "computer-implemented inventions", are patentable under certain conditions (in particular, they must meet the requirement of technical character).

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Collaborative improvements are a frequent source of dispute if the allocation of potential improvements has not been designed diligently enough. Partners with complementary expertise or products usually need access to collaborative improvements of their own expertise or products, which can be used independently from the other partner's expertise or products. Collaborative improvements that are inseparably linked to both partners' expertise or products usually require the development and negotiation of a new business model that can be structured as collaboration and licence agreements (that may include cross-licences), joint ventures, or co-marketing agreements.

7.2 What considerations apply in agreements between health care and non-health care companies?

Healthcare companies are used to a strict regulatory framework and they must require their partners to meet these requirements whenever they apply. Non-healthcare companies may be used to a much more liberal environment and overlook or underestimate regulatory requirements. Therefore, it is key that agreements do not only clearly allocate regulatory responsibilities, but also provide for adequate collaboration and control mechanisms that allow and incentivise the non-healthcare company to identify and meet relevant regulatory requirements in due time.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning is expected to dramatically improve prognosis and diagnostic accuracy. It is also expected that machine learning will displace significant parts of the work of radiologists and anatomical pathologists. These physicians focus largely on interpreting digitised images, which can be fed directly to algorithms instead. Massive imaging data sets, combined with recent advances in computer vision, will drive rapid improvements in performance. Radiologists and anatomical pathologists will become much more AI-literate to assure quality and further improve AI-based prognosis and diagnostic tools.

8.2 How is training data licensed?

Training data is rarely licensed on an exclusive basis, but digital health providers that obtain one of those rare exclusive licenses to quality training data will certainly have an advantage over the competition. Also, training data pools are often dynamic and further data will be added or data quality will be improved over time. Thus, for digital health providers, it is key to ensure that they get access to such amended or improved versions of training data. Finally, certain government entities, such as the Federal Office for the Environment, offer open access to digital data for AI applications.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

In Switzerland, copyright protection arises automatically upon creation of a work, regardless of any formality. Such a work must be an "intellectual creation" and must therefore have a human origin. As a result, a work generated by means of artificial intelligence (AI) will only be eligible for copyright protection if a human being is involved in the process of its creation. In addition, the authors of a work obtained with AI can only be humans who have provided creative inputs that are linked to and reflected in the final work. In that sense, a "creative causal link" must be perceptible between the creative work of the author(s) and the resulting work. The occurrence and extent of human intervention remains decisive in appreciating the authorship. Whether or not this is the case has to be assessed on a case-by-case basis. Authors may be, for example, individuals who provide the AI with decisive input in the process of creating a work by training a model to learn automatically or persons who have defined the goal to be achieved by the AI by specifically parameterising the AI.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Companies wishing to use data in machine learning have an interest in developing their AI systems with the best possible data. This creates a tension between their business interests and the legal data protection framework. As a result, the training data must be carefully selected. In addition, especially in the case of particularly sensitive personal data such as data on health or criminal prosecutions within the meaning of Art. 3 lit. c FADP, the ways in which the algorithm processes the data must stay within pre-defined limits. For example, it must be clarified whether the data may be further developed into complete data packages which could reveal additional sensitive information about the persons concerned.

Detailed quality data for use in machine learning is likely to have roughly the same commercial value as initial algorithms designed to solve a specific problem. Thus, we expect that whoever provides such detailed data on an exclusive basis for machine learning applications will negotiate for an important equity stake, upfront or milestone payments, royalties or other adequate compensation.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

There are no specific liability rules addressing digital health. The civil liability rules generally apply, in particular Art. 41 *et seq.* (liability in tort) and Art. 97 *et seq.* (contractual liability) of the Swiss Code of Obligations (no. 220) as well as the Federal Act on Product Liability (no. 221.112.944, as based on the European Union's Directive 85/374/EEC).

The basic prerequisites of liability in tort are:

- damage;
- illegality;
- causality between damage and illegality; and
- misconduct attributable to the defendant.

The basic prerequisites of contractual liability are:

- breach of contract;
- damage;
- causality between the breach and the damage; and
- misconduct attributable to the obligor.

Product liability according to the PLA:

- The "producer" is strictly liable for personal injuries and death as well as damage to property caused by a product which did not provide the safety which could reasonably be expected.
- There is a broad definition of "producer".
- An injured person may raise additional claims based on other legal grounds.

In addition, legal violations with digital health applications can lead to criminal sanctions and/or administrative disciplinary measures, which find their basis, *inter alia*, in the Therapeutic Products Act or Data Protection Act.

9.2 What cross-border considerations are there?

In international situations, the applicable law is determined by the Swiss Private International Law (CPIL; no. 291). Concerning torts, the international tort law includes product liability as well as personal injury. Articles 134-139 CPIL provide special conflict-of-law rules for these specific categories of torts. In the case of such special tort, it must also be questioned whether a subsequent choice of law according to Art. 132 CPIL is permissible. If the parties do not choose the law and if there is no specific tort pursuant to Articles 134-139 CPIL, the law applicable to the pre-existing legal relationship between the counterparties (Art. 133 para. 3 CPIL) may be considered. If no such pre-existing relationship exists, and the damaging party and injured party have their habitual residence in the same country, the law of this country is applicable according to Art. 133 para. 1

© Published and reproduced with kind permission by Global Legal Group Ltd, London

CPIL. Only as the last possible connection does the traditional general principle of the connection to the place of tort (*lex loci delicti commissi*) come into play (Art. 133 para. 2 CPIL).

With regard to punitive, exemplary, moral or other non-compensatory damages, which are not available under Swiss law, Swiss courts refuse to award such damages even if the applicable foreign law provides for such damages (cf. Article 135 II CPIL).

The Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (no. 0.275.12) regulates the jurisdiction, recognition and enforcement of judgments between the Member States of the European Union, Switzerland, Norway and Iceland.

In contrast to civil law, the Swiss administrative law does not provide for specific conflict of law rules. The principle of territoriality applies: a situation occurring in a given territory must be assessed by the competent authorities of that territory in accordance with the law applicable there, and any exercise of sovereign powers or the use of coercive means is reserved to the relevant organs of the state, unless there are different intergovernmental arrangements.

International criminal law distinguishes between the principle of active personality (applicability of the law of the State of which the offender is a national) and the principle of passive personality (applicability of the law of the State of which the victim is a national). According to the real or protective principle, the law of the State whose interests have been harmed by the crime is to be applied; this is a special case of the effect principle.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

In healthcare, patient data is subject to medical professional secrecy. "Swiss Cloud" providers based in Switzerland are also covered by Art. 321 of the Swiss Penal Code as vicarious agents of the physician or other medical professional. Thus, medical professional secrecy is maintained.

Patient data can be stored with foreign cloud providers if these cannot read the patient data (i.e. the patient data is encrypted and the cloud providers do not have the key). Technically, this requires that the patient data is encrypted in Switzerland before being transferred to the foreign cloud.

Finally, certain health data might not qualify as patient data covered by the medical professional secrecy. Digital health providers may process such data in Swiss or foreign cloud-based services subject to the usual data protection requirements. This might include, in particular, stating explicitly that these applications or uses are not intended for patient data covered by medical professional secrecy.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Non-healthcare companies entering the digital healthcare market must become familiar with the extensive regulatory requirements in the healthcare sector and integrate the cost of compliance in their business models. For example, if an app is subject to medical device regulation, increased requirements for quality management and documentation apply to development, programming, validation, testing and version management. A market launch in Switzerland also requires a CE mark and, in most cases, must be reported to Swissmedic.

At the app developer's expense, Swissmedic may carry out checks to determine whether an app qualifies as a medical device and whether the conditions for placing it on the market are met. If these conditions are not met, Swissmedic may withdraw the app from the market and prohibit further marketing in Switzerland and the EU.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

When looking at the business model of a digital healthcare venture, a key issue is whether the venture's final product or service will be reimbursed by national health insurance plans, sold to patients without such reimbursement, sold to healthcare providers such as hospitals, or marketed to pharmaceutical or medical device companies to enhance their existing products or services. Another key issue is how the venture stands out from the competition, i.e. if there is solid patent, trademark or copyright protection or whether the concept is to be faster and better than the (potential) competition.

Legal issues to consider during due diligence are: who developed and who owns which parts of the software; who tested the software with what kind of data; and whether real-life data was used in the tests as well. Further legal issues are timing and costs for the regulatory pathway to comply with healthcare and data protection legislation.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Dr. Stefan Kohler has extensive experience in IP/technology law and regulated markets such as healthcare, pharma, medtech, biotech, cosmetics and foodstuffs. He regularly represents Swiss and foreign companies before Swiss courts and administrative authorities. He first studied science at the ETH in Zurich which enables him to accurately and legally classify technical-scientific facts.
Stefan is an associate judge at the Swiss Federal Patent Court, president elect of the board of the Swiss Licensing Executives Society (LES), board member of BioLawEurope, board member of Swiss Healthcare Startups (SHS) and a member of the Forum for Genetic Research of the Swiss Academy of Sciences. He is a lecturer at the entrepreneurship program to boost the success of eHealth companies at the Università della Svizzera Italiana (USI) and teaches aspiring patent attorneys at the Swiss Institute for Intellectual Property in the field of licensing agreements, R&D agreements and technology transfer.

VISCHER AG
Schuetzengasse 1
P.O. Box
8021 Zurich
Switzerland

Tel: +41 58 211 34 19
Email: skohler@vischer.com
URL: www.vischer.com

Christian Wyss specialises in drafting and negotiating contracts for clients from the Life Sciences and Information Technology industries. Christian has extensive experience with technology transfer and licence agreements, research, development or marketing co-operations, clinical trial agreements, contract manufacturing agreements and distribution agreements. He regularly works with clients in financing rounds, acquisitions, or joint ventures and assists with intellectual property related issues in M&A transactions. Christian also advises on implementing compliance with the Swiss data protection laws.
Christian's clients range from start-ups, over VC financed development stage companies, to industry leaders. Christian is familiar with balancing each project's technology driven aspects and the requirements of industry partners, investors, or other constituencies.
Christian received his law degree from the University of Basel, Switzerland, and his LL.M. from Wake Forest University School of Law in Winston-Salem, North Carolina. He was admitted to the Bar in Switzerland in 2002.

VISCHER AG
Aeschenvorstadt 4
P.O. Box 329
4010 Basel
Switzerland

Tel: +41 58 211 33 39
Email: cwyss@vischer.com
URL: www.vischer.com

As a leading Swiss corporate law firm, VISCHER advises and represents enterprises and entrepreneurs in all aspects of commercial law both in a domestic and a global context. VISCHER's more than 100 attorneys, tax advisors and notaries are organised in practice and sector groups that are fully integrated and work across offices located in Switzerland's most important business centres: Zurich, Geneva and Basel. VISCHER combines legal competences and practices with in-depth expertise in particular industries. VISCHER's specialised practice groups are always focused on understanding the business and the specific problems and challenges faced by clients. The VISCHER Life Sciences Team and the VISCHER IP/IT Team are dedicated to the special legal issues in the field of digital health. The VISCHER Life Sciences team is the largest practice group of this kind in Switzerland focusing on regulatory matters, including compliance and administrative procedures, and support clients from initial start-up to ongoing development and eventual sale, merger or IPO. The VISCHER IP/IT team supports clients in the development and implementation of IP strategies, litigation, proceedings and transactions in all areas of intellectual property and IT law.

www.vischer.com

VISCHER

© Published and reproduced with kind permission by Global Legal Group Ltd, London

United Kingdom


Sally Shorthose


Philippe Bradley-Schmieg


Toby Bond


Ben King

Bird & Bird LLP

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

Apps, programmes and software used in the health and care system – either standalone or combined with other products such as medical devices or diagnostic tests.

1.2 What are the key emerging technologies in this area?

Digitised health systems – in particular, the wholesale digitisation of patient data and prescription delivery in the UK National Health Service ("**NHS**").

mHealth – apps on mobile and connected wearable devices to monitor and improve health and wellbeing.

Telemedicine – delivery of health data from mHealth apps to the patient's clinician, and the provision of distance support to patients either through healthcare practitioners or AI; the integration of telemedicine services with digitised health systems.

Health data analytics – the digital collation, analysis and distribution (including on a commercial basis).

1.3 What are the core legal issues in health care IT?

The two core legal issues are:

- compliance, in the digital collation and handling of patient data, with the requirements of the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and the UK Data Protection Act 2018 ("**DPA**"); and
- compliance, in delivering telemedicine services, with the UK healthcare regulatory regime – which is not yet fully updated to deal with the issues arising from the delivery of telemedicine services.

2 Regulatory

2.1 What are the core health care regulatory schemes?

England, Scotland, Wales and Northern Ireland each have their own regulatory regime and competent authority. In England (approximately 85% of the UK population), the relevant legislation is the UK Health and Social Care Act 2008. Broadly equivalent legislation and regulators are in place in the other UK nations. All national regimes require all providers of regulated healthcare services (including e.g. telemedicine) to meet the requirements of the applicable legislation and to register with the relevant national regulatory body in order to be able to legally undertake those services.

Medicines and healthcare products (including software as a medical device) are governed across the UK by the UK Human Medicines Regulations 2012, the UK Medical Device Regulations 2002 ("**MDR 2002**") and the EU Medical Device Regulation (EU) 2017/745 ("**EU MDR**"). Note that once EU law (including the EU MDR) ceases to apply in the UK after Brexit, it is intended that the MDR 2002 will be updated to be generally aligned with the provisions of the EU MDR.

2.2 What other regulatory schemes apply to digital health and health care IT?

The use of personal data in digital health is regulated primarily by the GDPR, the DPA, and laws on confidentiality that vary between the different parts of the UK (England, Northern Ireland, Scotland and Wales).

2.3 What regulatory schemes apply to consumer devices in particular?

Consumer health devices are, to the extent they are "medical devices", covered by the MDR 2002 and the EU MDR. All medical devices need to meet the applicable CE marking requirements in these regulations and must be registered.

All consumer devices are regulated by the UK General Product Safety Regulations 2005 and those other CE marking regulations which apply to the specific product, e.g. UK Electrical Equipment (Safety) Regulations 2016, etc. Evidence of compliance with applicable CE marking laws and regulations must be compiled and maintained by a nominated responsible person in the EU (after Brexit, the UK). Once EU law ceases to apply after Brexit, the UK will implement its own "UKCA" mark, and the UK CE marking regulations will be updated accordingly.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

For the healthcare regulatory regimes in the four nations, the relevant regulatory authorities are:

- England – Care Quality Commission.
- Scotland – Healthcare Improvement Scotland.
- Wales – Healthcare Inspectorate Wales.
- Northern Ireland – The Regulation and Quality Improvement Authority.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

The Medicines and Healthcare product Regulatory Agency ("**MHRA**") is the competent regulatory authority for medical devices and maintains the register of such devices.

Various regulatory bodies have responsibility for particular UK CE marking regulations (and will retain this responsibility for the "UKCA" marking scheme).

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

Primary areas of concern:

- Telemedicine service providers: Loss of registration (and thus loss of ability to legally provide healthcare services) for failing to comply with the relevant standards. Serious criminal conduct may result in prosecution and significant fines.
- Medical devices (including software): Failure to comply with the relevant regulations can result in the product being recalled and withdrawn from market by the MHRA, and, if there is serious failure to comply with the regulations, an unlimited fine and/or six months imprisonment on conviction.
- In general: Privacy and data security.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Software as a medical device is governed by the MDR 2002 and (until the Brexit process is completed) the EU MDR.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  - Determining whether any of the devices used qualify as medical devices.
  - GDPR compliance – appropriate notice and consent practices; implementation of necessary security measures; and ensuring that algorithms are robust and unbiased.
  - Contractual issues between the various suppliers of services and devices.
  - If telemedicine is included, compliance with the local pharmacy and prescribing rules and regulations will be necessary.
- **Robotics**
  - Liability allocation for poor outcomes – designer, manufacturer, HCP or even power supplier.
  - Compliance with Regulations: e.g. for waste electrical and electronic equipment (WEEE).
  - Compliance with MDR 2002/EU MDR.
  - Data protection.
- **Wearables**
  - Determining whether any of the devices used qualify as medical devices.
  - GDPR compliance – securing appropriate consent from data subjects, implementation of necessary security measures, and retention of necessary information.
  - Contractual issues between the various suppliers of services and devices.
- **Virtual Assistants (e.g. Alexa)**
  Similar issues as for Telehealth.
- **Mobile Apps**
  Similar issues as for Telehealth.
- **Software as a Medical Device**
  Compliance with MDR 2002/EU MDR.
- **AI-as-a-Service**
  Similar issues as for Telehealth.
- **IoT and Connected Devices**
  Similar issues as for Telehealth.
- **Natural Language Processing**
  No particular issues.

3.2 What are the key issues for digital platform providers?

Data protection and especially the transmission, storing processing and use of data – and ensuring adequate consent to such use has been obtained.

With Brexit on the horizon it is unclear how the position regarding the movement of data in and out of the UK will arise.

The digital platform provider must ensure, to the extent it is responsible, that advice and services provided on the platform are fit for purpose as failure to process information resulting in personal injury may result in liability.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

- Whether or not (explicit) consent should be used as the basis for personal data processing. This is an area where there is likely to be movement in the near future.
- Determination of whether relevant data is personal data or has been sufficiently anonymised. In the case of de-identified data, the answer is not always clear cut.
- Identifying whether data is *concerning health* (and subject to more stringent rules, as is genetic, biometric and sex-related data), *versus* less sensitive data that might for instance be collected for wellness purposes (e.g. step counts, sporting performance, etc.).
- At least in the short term, Brexit is not expected to substantially change the main privacy and data security requirements applicable to digital health in the UK.

4.2 How do such considerations change depending on the nature of the entities involved?

There is a significant distinction between use of data within *versus* outside the NHS; the impact of "soft law", such as restrictions deriving from NHS policy and "Directions" issued by the UK Secretary of State, will be more acutely felt when working with NHS-originating data, compared to data in (or sourced from) private healthcare or consumer settings.

Even in public sector contexts, the rules differ between different parts of the UK. An important example is the "National Data Opt-out", a scheme allowing NHS patients to easily opt out from certain secondary uses of their personal data in England. This does not apply to patient data from Northern Ireland, Scotland or Wales.

4.3 Which key regulatory requirements apply?

The use of personal data in digital health is regulated primarily by the GDPR, the DPA, and laws on confidentiality that vary

© Published and reproduced with kind permission by Global Legal Group Ltd, London

between the different parts of the UK (England, Northern Ireland, Scotland and Wales).

In addition, a substantial body of "soft law" tends to be imposed by healthcare regulators, NHS bodies, and other stakeholders' policies and contracts.

Additional legislation can apply for specific data uses, e.g. the Privacy and Electronic Communication Regulations, "**PECR**") for access to and storage of data on Internet-connected devices is also restricted by PECR. Medical device or clinical trial laws further limit the use of personal data.

- The GDPR imposes significant restrictions on the use of health data without providing notice of that use and obtaining explicit consents from individuals.
- Operators in England and Wales (in particular) must also deal with more restrictive requirements of "common law", particularly surrounding confidentiality and misuse of private information ("**MoPI**"). Without consent (which for these purposes could be implied or explicit), or a clear statutory permission, only uses of patient personal data that are necessary in the public interest, are permitted under English and Welsh law on confidentiality and MoPI.
- GDPR/DPA also impose additional requirements, including to keep data secure, maintain its availability and accuracy, report data incidents, appoint a Data Protection Officer and/or a "Representative", conduct risk assessments, and generally, ensure that usage of personal data is "fair" and does not involve excessive amounts of data.
- GDPR grants individuals substantial personal data rights, e.g. to access or delete their data. The DPA adds certain additional rules, including criminal offences for re-identifying personal data, or selling it after it has been improperly obtained.
- DPA also adds additional conditions (beyond those in the GDPR) on use of personal data for significant automated decision-making that has legal or "substantially similar" effects on an individual. This will need to be borne in mind as software (e.g. AI) becomes increasingly capable of replacing (rather than merely supporting) human decision-making in healthcare settings.

4.4 Do the regulations define the scope of data use?

GDPR/DPA generally prohibit the use of health-related personal data without prior, explicit consent, but list exemptions from that restriction – e.g. use of personal data to provide healthcare (by or under the responsibility of a person bound by a duty of confidentiality) is permitted. Similarly, they allow non-consensual scientific research in the public interest (provided that such research does not entail the taking of decisions affecting the relevant individual(s), unless the project has ethical committee approval).

However, as noted in question 2.2 above, there are supervening restrictions under contract, soft law and confidentiality/MoPI rules. Care should be taken (and specialist advice obtained) to ensure that, where relying on GDPR/DPA exceptions, these restrictions do not apply to the use of personal data.

4.5 What are the key contractual considerations?

Digital health companies will often find themselves subject to heavy requirements imposed by NHS customers. Organisations not dealing with the NHS will often have greater freedom to operate.

More generally, a key consideration for the design and negotiation of contracts is whether for GDPR purposes the different parties are "processors" or "controllers" of the data – and in the latter case, whether two or more parties are "joint" or "independent" controllers. That classification will dictate the GDPR-imposed terms that must be included in the contract, and also inform each party's compliance strategy and required risk protections (indemnities, warranties, due diligence, and insurance).

If personal data is leaving the European Economic Area, then the GDPR will often require that additional contractual terms (typically based on a preapproved set of "standard"/"model" contractual clauses) must be put in place between the data's exporter(s) and importer(s).

By contrast, UK data protection laws generally have little impact on contracts *with individuals*; the law is generally clear that data protection-related matters should be dealt with *outside* of those contracts (e.g. through dedicated privacy notices, and stand-alone consent requests, e.g. via pop-up banners or "user settings" pages on websites or in apps).

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The sharing of personal data, rather than its mere use within a single organisation, means that confidentiality and privacy concerns will often be more acute than simply using data. For example, in England and Wales, even greater attention needs to be paid to the existence of consent, statutory permission and/or a public interest justification for the proposed data sharing. To complicate matters, that legal basis might be different for the different parties, and thus subject to differing restrictions and conditions.

Sharing personal data also introduces potentially significant counterparty risk: both parties to a data sharing arrangement might face legal risk even if just one of the parties misuses the data. Due diligence, contracting and clear compliance arrangements are therefore important.

Finally, key aspects of the data sharing may need to be explained to individuals, in accordance with the GDPR's transparency obligations.

5.2 How do such considerations change depending on the nature of the entities involved?

As with data use, key legal variations tend to be driven by differences in the purpose of data sharing, not the nature of the entities involved. That said, certain public sector entities (particularly, those within the NHS) might have specific legal powers – or restrictions – regarding data sharing and the performance of their public duties. This could also vary depending on their location within the UK.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Preceding answers, in particular for questions 4.1, 4.3, 4.5, 5.1 and 5.2, have covered the key regulatory requirements applicable to the sharing of personal data in a digital health context.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

6 Intellectual Property

6.1 What is the scope of patent protection?

Monopoly patent protection is available for novel, non-obvious products or processes which have industrial application. Fees payable on application and renewal. Protection lasts 20 years from date of application, once the patent is granted (see UK Patents Act 1977).

6.2 What is the scope of copyright protection?

Right to prevent copying, dealing in copies, issuance of copies to the public, performance, broadcast, or adaptation for (relevant works only):

- Literary, musical, artistic works (including software) – life of author plus 70 years.
- Published sound recordings – 70 years from date of publishing.
- Broadcasts – 50 years from date of broadcast.

Copyright (generally) arises on creation and fixation of the work, with no requirement for registration. (See UK Copyright, Designs and Patents Act 1988 (the "**CDPA**").)

6.3 What is the scope of trade secret protection?

Common law of confidence protects trade secrets. It protects information which:

- has a quality of confidence;
- is disclosed under an express or implied obligation of confidence; and
- is used or further disclosed in an unauthorised manner.

The UK Trade Secrets (Enforcement, etc.) Regulations 2018 also prevent acquisition, use or disclosure of trade secrets where this would constitute a breach of confidence in confidential information. However, the common law of confidence provides stronger and more comprehensive protection.

6.4 What are the typical results on academic technology transfer rules?

IP rights in technology developed in academic institutions usually vests in the academic institution. The institution will typically seek to licence the technology either to existing businesses, or via the creation of a spin-out company to commercialise the technology.

There are no specific laws governing academic technology transfer.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Software is only patentable in the UK to the extent that it meets the requirements in the UK Patents Act 1977. These requirements are stringent and difficult to meet for software. Generally, however, software will be protected as a literary work under the CDPA (see question 6.2, above).

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

It is often suggested that joint ownership of IP/improvements is the fairest way of approaching collaborations. The downside of this blanket approach is that treatment of jointly owned IP varies from jurisdiction to jurisdiction and also by IP right, so the joint owner might find himself/herself in an invidious situation if complete clarity is set out regarding the permitted uses a joint owner may have over the IP.

There are better ways of approaching this – have ownership following the ownership of background on which the improvement is made or assign it in accordance with predetermined fields of use. Royalty payments and licences to background technology should also be provided for.

7.2 What considerations apply in agreements between health care and non-health care companies?

As with any agreement, the allocation of rights and obligations should be set out, especially in relation to liability. It is likely that the parties will have responsibilities related to their respective expertise, and these should be specified, as well as responsibility for data protection compliance.

Public sector healthcare providers often have very strict rules (even to the extent of bureaucracy) which can mean that negotiation of IP rights, for example, can be difficult to deviate from the norm.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

The statistical and pattern recognition capabilities of machine learning have a wide range of possible applications in the digital health context. These encompass activities which are trivial for any human to complete but challenging for traditional computer systems (e.g. converting handwritten medical records into text) and those which require many years of human expertise (e.g. detecting breast cancer in mammograms). Their use also covers the full range of potential medical purposes from diagnosis, prevention, monitoring, prediction and prognosis of disease to its treatment and alleviation. Applications currently receiving particular attention are the use of pattern recognition techniques to detect abnormalities in medical imaging data. However, any digital health problem which involves the identification of signals in a noisy environment is potentially susceptible to the use of machine learning.

Machine learning can also be applied to the manner in which digital health services are delivered. Natural language processing can, for example, be used to facilitate human interaction with systems which are themselves based on machine learning techniques. Potential applications include "chat bots" combined with expert diagnostic systems to replicate a doctor's consultation. Current systems are limited to diagnosing specific conditions in tightly controlled situations. Future systems will generalise this approach to broader diagnostic platforms with general application.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

8.2 How is training data licensed?

Under English law there is no single property right which applies to data *per se* and there is a general reluctance to treat information as a form of property. There may however be legal rights which may, depending on the nature/source of the data, be used to control access to, use, and disclosure of training data. These include rights in confidential information along with IP rights in the data elements (e.g. copyright, where applicable) or in an aggregation of data (e.g. copyright in original databases or EU database right).

Where these rights exist they can form the subject matter for a contractual licence to training data, e.g. an IP licence and/or knowhow licence. The English courts have also recognised that it is possible to impose contractual restrictions on access to, use and disclosure of data even where that data is not protected by other rights. Training data can therefore also be licensed on a purely contractual basis under English law. The possibility of granting a purely contractual licence does not however give rise to some general right of "ownership" in the data being licensed. Unless they refer to intellectual property rights in the data, reference to "ownership" of data in licences may give rise to confusion as this term has no clear legal meaning under English law. Well-drafted data licences will commonly focus on the rights and restrictions regarding access, use and disclosure of the data and will only refer to ownership in the context of intellectual property rights in the data. They will also address (often complex) issues relating to access, use and disclosure of derived data which is created by the licensee using the licensed data.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Under English law, algorithms are potentially protectable by copyright as original literary works. Where an algorithm is written by a human, the author of that work is the person who creates it (Section 9(1) CDPA). This is taken to be the person responsible for the protectable elements of the work, being those elements which make the work "original" (i.e. those parts that are the "author's own intellectual creation").

First ownership of a work and the duration of the protection available are defined with reference to the author. However, where an algorithm is written using machine learning without active human involvement, it may not be possible to identify a human who can be said to have created the work, i.e. there is no human author such that the work qualifies as "computer generated" under Section 178 CDPA. In these circumstances Section 9(3) CDPA deems that the author of the work is the "person by whom the arrangements necessary for the creation of the work are undertaken". This can potentially be one or more natural or legal persons. Under section 12(7) the duration of protection of a computer-generated work is 50 years from the end of the calendar year in which it is created.

While the test set out in Section 9(3) CDPA determines the identity of the author of a computer-generated, work it is not currently clear as a matter of English law whether such work will actually qualify as copyright work. Under Section 1(1) CDPA, copyright only subsists in *original* literary works, which requires an intellectual creation by the author which reflects an expression of their personality. It is questionable whether an algorithm developed by machine learning without human involvement could be said to be an intellectual creation reflecting the personality of the person making the arrangements necessary for its creation. As a result, such an algorithm may not qualify for copyright protection under English law. An alternative view is that Section 9(3) CDPA in fact creates its own *sui generis* right for computer generated works which is not subject to the usual requirement for originality. These issues have not thus far been addressed by the English courts and claims to copyright (or an absence of rights) in algorithms developed by machine learning without human intervention must therefore be treated with caution.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Many machine learning projects often involve collaboration between a party with expertise in deploying machine learning and another party with access to the data required to train a machine learning system to solve a particular problem. Common commercial issues which arise in this context include the rights each party obtains in the resulting system, e.g. can the resulting system be resold to others or adapted for purposes which go beyond those originally envisaged.

Similar considerations apply to the future use and disclosure of the training data itself, e.g. is the recipient allowed to retain the data after the project is complete and can it be re-used for other purposes (either in its original form or in some aggregated/derived form) and/or shared with third parties (and if so under what terms)? Where the data is provided on a long-term basis with a defined scope of use, the licensor may wish to include audit rights to ensure the data continues to be used and disclosed in compliance with the terms of the licence.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

Liability for adverse outcomes in digital health is governed both by the law of contract (where services are not delivered in accordance with a contract) and by the common law of negligence where, whether or not a contract is in place, a duty of care exists between parties, and a breach of that duty (by falling below the reasonable standard expected in carrying out that duty) causes loss (including personal injury).

Additionally, the UK Consumer Protection Act 1987 (the "**CPA**") sets out a strict liability regime for consumer products, including medical devices. In summary, under such claims a claimant does not need to show any fault on the part of the defendant. Instead, a claimant needs to demonstrate: (i) the presence of a defect in a product according to an objective standard of safety as reasonably expected by the public; and (ii) a causal link between that defect and the loss suffered.

Finally, the GDPR might create joint and several liability between partnering organisations if GDPR noncompliance led to an adverse outcome – for example, basing clinical decisions on inaccurately-recorded patient data or a biased algorithm.

9.2 What cross-border considerations are there?

Under currently-applicable EU law (the Rome Regulations), generally, UK national (English and Welsh, Scottish or Northern Irish) law will apply to non-contractual (e.g. personal injury) and contractual claims based on digital health delivery to consumers/patients in the UK, whatever the country of origin of the provider. The situation is not expected to change significantly post-Brexit.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Key issues include (i) data security, (ii) commercial re-use of the data by the Cloud provider, and (iii) whether data will leave the UK.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

It is a complicated and heavily regulated area, and these regulations can vary from jurisdiction to jurisdiction – no broad brush approach will be applicable. It is also a fast-moving market and keeping up with the changes in regulation is essential.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

When considering a target:

- Ensure that procedures are in place for compliance with relevant areas, especially data protection, MDR and WEE.
- Consider competition – are they first, second or third to market?
- Consider patent protection – has this been secured where applicable and have they taken steps to protect and exploit unregistrable IP, such as trade secrets.
- Do they own all necessary IP?
- Do they have good supply and service contracts in place, and secure sources of hardware?

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Sally Shorthose is a partner in the Life Sciences and Intellectual Property Group at Bird & Bird LLP, based in London. Before her return to private practice in 2001, she had spent 11 years working in-house in senior roles in the Life Sciences industry, including several years as Legal Director of the Novartis Group in the UK. She now specialises in transactional IP work and life sciences regulatory work. She is the editor of the Kluwer Law publication, the EU Guide to Pharmaceutical Regulatory Law and is a regular speaker internationally on all types of IP and regulatory issues. She has spent much of the last three years leading the Brexit advisory team at Bird & Bird.
Solicitor – England & Wales, 1988.
Solicitor – Ireland, 2017.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7982 6540
Email: sally.shorthose@twobirds.com
URL: www.twobirds.com

Philippe Bradley-Schmieg is an associate in Bird & Bird's International Privacy and Data Protection group. He has extensive experience advising clients on privacy and data security requirements, in particular the EU's GDPR, and UK and EU e-Privacy rules.
His practice covers advisory, public policy, transactional and contentious work, particularly in areas such as life sciences (pharma, biotech and medical devices), eHealth, mHealth, telecoms and the use of cloud computing and AI in regulated sectors.
He participates in the Global Alliance for Genomic Health (GA4GH)'s GDPR working group, the Future of Privacy Forum (FPF)'s Health working group, and FPF's Corporate-Academic Data Stewardship Research Alliance (CADRA). Before joining Bird & Bird in 2018, he spent over five years working with a US law firm, including four years in its Tier 1 EU data protection practice.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7415 6691
Email: phil.bradley@twobirds.com
URL: www.twobirds.com

Toby Bond is a senior associate in Bird & Bird's Intellectual Property Group, based in London. Much of his work focuses on helping clients navigate issues relating to the protection and commercialisation of data as they take advantage of the power of big data analytics and artificial intelligence. He has a particular interest in the wider intellectual property issues arising from the development and deployment of AI systems. Toby also advises clients on medical devices legislation and his broader experience covers CE marking, EU batteries legislation, REACH/CLP, RoHS, WEEE and Electromagnetic Compatibility, with a particular focus on emerging technologies including IoT and AI.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7415 6718
Email: toby.bond@twobirds.com
URL: www.twobirds.com

Ben King is an IP and regulatory lawyer at Bird & Bird. He has a broad practice encompassing life sciences, tech and general regulatory and transactional work, and has significant experience in advising on UK CBD and medical cannabis regulation. He has also assisted on several IP disputes, including *Warner Music & Sony Music v TuneIn* (2019). He has undertaken secondments with a biotech company, a generic pharmaceutical company, and an international bank.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 3017 6991
Email: ben.king@twobirds.com
URL: www.twobirds.com

Bird & Bird is an international law firm which focuses on helping businesses being changed by technology and the digital world. It has over 1,300 lawyers and legal practitioners in 30 offices worldwide.
Our International Life Sciences & Healthcare group works with over 50% of the world's largest pharmaceutical, biotechnology and medical devices companies. We have the largest patent litigation group in Europe and are recognised by major global directories as a top tier life sciences firm.
Our focus on business being changed by technology and the digital world enables us to support our clients operating in this rapidly changing environment. Our multidisciplinary team of 240 specialist life sciences and healthcare lawyers worldwide can advise you on every aspect of the business cycle of a life science and healthcare product or service, from incorporation through development, to protection and exploitation of intellectual property.
www.twobirds.com

Bird & Bird

© Published and reproduced with kind permission by Global Legal Group Ltd, London

USA


William A. Tanenbaum


Michael Gaba


Eric J. Hanson


Erica Beacom

Polsinelli PC

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

Digital Health is the application of computer technologies, platforms and software for use by health systems, clinicians, researchers, payers, patients and individuals to advance healthcare (such as clinical treatment) and for wellness (such as fitness apps). Digital Medicine is generally considered a subcategory. Digital Health uses machine learning and data analytics across the spectrum of healthcare.

1.2 What are the key emerging technologies in this area?

The key-emerging technologies are as follows:

- Electronic health records and related technologies that record, analyse, integrate and transfer health data.
- Telemedicine and remote healthcare solutions, which will be enhanced by the faster speed and greater bandwidth of 5G (fifth-generation) wireless networks. (Please see the chapter in this book entitled "Digital Health, New Technologies and Emerging Legal Issues" for further discussion of 5G.)
- Artificial Intelligence, machine learning, natural language processing and data analytics.
- Digital Fabrics for generating rich data streams for machine learning.
- Edge computing to avoid the latency of cloud computing.
- Mobile apps and self-generated analytics for wellness and health.

1.3 What are the core legal issues in health care IT?

The core legal issues are as follows:

- Data protection, security and privacy compliance in accordance with HIPAA (the Health Insurance Portability and Accountability Act) and the HITECH Act (the Health Information Technology Economic and Clinical Health Act of 2009), as codified at Title 42 U.S.C. [United States Code] § 1320d *et seq.*, as well as various state laws such as the California Consumer Privacy Act (CCPA).
- Medical device regulatory compliance generally under the jurisdiction of the Federal Food and Drug Administration (FDA). The FDA exercises jurisdiction under the Federal Food, Drug and Cosmetic Act (Title 21 U.S.C. Chapter 9).
- Telemedicine and remote regulatory compliance, which is an area where the regulatory framework is evolving.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The core regulatory schemes are as follows:

- Regulations of the federal Department of Health and Human Services (HHS) including its agency, the Centers for Medicare and Medicaid Services (CMS), which regulates Medicare (Title XVIII of the Social Security Act (42 U.S.C. [United States Code] §1395-1395ccc)) (chiefly for older patients) and Medicaid (Title XIX of the Social Security Act (42 U.S.C. §1396 *et seq.*)) (generally for lower income patients).
- "HIPAA", the Health Insurance Portability and Accountability Act of 1996, and the HITECH Act, the Health Information Technology for Economic and Clinic Health Act, governs the privacy and security of protected [personal] health information (PHI) including when transmitted in electronic form (ePHI), as codified at Title 42 U.S.C. § 1320d *et seq.*
- The CCPA governs the privacy and security of personal information relating to California residents. Although personal information protected by HIPAA is excluded, CCPA applies to organisations which do not fall within the definition of "covered entities" under HIPAA, as well as to categories of personal information which do not constitute (and are not protected as) PHI.

2.2 What other regulatory schemes apply to digital health and health care IT?

Other regulatory schemes are as follows:

- The 21st Century Cures Act, which defines software functionality that falls within and outside of FDA jurisdiction for medical devices.
- FDA regulations applicable to digital health products that meet the statutory requirements as defined in Section 201(h) of the Federal Food, Drug and Cosmetic Act, as amended (codified at Title 21 U.S.C. §321(h)), including software as a medical device (SaMD) and regulations applicable to health app development. The regulatory authority of the Federal Trade Commission (FTC) applies over advertising and claims made for software-based digital health products that qualify as wellness products, which are excluded from FDA jurisdiction.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.3 What regulatory schemes apply to consumer devices in particular?

Those of the FTC as discussed in question 2.2.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The principal regulatory authorities are as follows:
- HHS and its agencies including CMS; certain enforcement proceedings are brought by the US Department of Justice.
- The FDA, as discussed in question 2.2 and also with respect to mobile apps where the intended use is to assist in prevention, treatment, mitigation and cure diseases and medical conditions. FDA jurisdiction includes registration and listing requirements and quality system regulations (21 CFR [Code of Federal Regulations] Part 820).

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The key areas of enforcement are as follows:
- Data privacy and security violations under HIPAA/HITECH and state laws (including CCPA).
- Loss of a licence or ability to practise medicine, operate a facility, or market/commercialise a product/service.
- Inability to participate in or receive funds related to government programmes, including Medicare and Medicaid.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

SaMD is regulated by the FDA as discussed in question 2.2. Higher-risk clinical-related SaMD may require clinical trials and approvals. Clinical use raises complex issues under US law. The FDA does not regulate the practice of medicine: that occurs at the state level.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

The core issues that apply to digital technologies are:
- **Telehealth**
  - Medical licensing requirements relating to the location of the patient and the healthcare provider, including the corporate practice of medicine issues.
  - Medical device regulations.
  - Data privacy including the applicability of HIPAA authorisations (an issue which generally applies to the technologies below).
- **Robotics**
  - Surgical assistance.
  - Remote physical examination in remote areas.
  - Combination of technologies from multiple suppliers.
  - Telecommunications and wireless network.
  - Device malfunctions.
- **Wearables**
  - Whether it is a wellness/fitness device or must be certified as a medical device.
  - Integration with apps (and potential different vendor).
  - Federal Communications Commission (FCC) transmission regulations.
  - Data transmission and privacy.
  - Combination into a Body Area Network.
- **Virtual Assistants (e.g., Alexa)**
  - Whether the vendor is a business associate (as Amazon is for Alexa) (see business associate discussion in question 4.2).
  - Privacy concerns where the vendor listens to user voice recordings.
- **Mobile Apps**
  - Whether an app is a FDA-regulated SaMD.
  - Whether the app developer is a business associate.
  - Consent requirements.
- **Software as a Medical Device**
  - FDA SaMD rules.
  - Intellectual property (IP) ownership and licensing.
- **AI-as-a-Service**
  - AIaaS is a machine learning service calibrated for a specific function, such as facial recognition.
  - AIaaS also can be a generalised machine learning framework that can be customised for a variety of uses.
  - Potential bias in algorithm and impact on diagnoses.
  - Risk if AIaaS is a "black box" and the weight given by the algorithm to specific factors is often unknown.
- **IoT and Connected Devices**
  - Data privacy and security.
  - IT security and breach vulnerability.
  - Edge computing (computing that occurs at the "edge" of a connected device network) to avoid the latency of cloud computing.
- **Natural Language Processing**
  - Validation of results.

3.2 What are the key issues for digital platform providers?

The key issues for digital platform providers are as follows:
- Privacy and data protection for the data.
- Obtaining the required data consents and compliance with the HIPAA Privacy and Security Rules for data protection, as well as other applicable laws such as CCPA.
- Whether they are business associates (see question 4.2) or service providers under CCPA.
- Commercial and IP provisions in agreements.
- As of the publication date, the proposed rule for the "Trusted Exchange Framework and Common Agreement" ("TEFCA"), which is promulgated by the Office of the National Coordinator for Health IT (part of HHS), is intended to increase interoperability between Health Information Networks, which remains subject to rule-making procedures.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The key issues to consider for use of personal data are:
- Whether personal data is also protected health information subject to HIPAA or whether it relates to wellness

© Published and reproduced with kind permission by Global Legal Group Ltd, London

which is not subject to federal healthcare regulations but would instead be subject to CCPA. Fitness and sports performance are examples of wellness data.
- Whether regulatory consents are required and if so, what is required to meet them.
- The statutory status and nature of the entities collecting and using the data subject to FTC jurisdiction.

4.2 How do such considerations change depending on the nature of the entities involved?

Under HIPAA/HITECH, an entity may qualify as a "covered entity" if it is a healthcare provider, healthcare clearinghouse, or health plan that conducts standard administrative and financial transactions in electronic form. A "business associate" is a person or entity that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involves the creation, receipt, maintenance and transmission of PHI. PHI may be exchanged between a covered entity and its business associate, but there must be a valid Business Associate Agreement (BAA) between the two parties.

If the entity is a provider of fitness or wellness apps, then it is generally not a covered entity but it may be acting as a business associate, and other state laws, such as CCPA, may apply.

Under the HIPAA Privacy Rule, a limited set of identifying data can be shared by covered entities with researchers who are not covered entities for the purposes of research, healthcare operations and public health activities, without prior patient consent, provided a Data Use Agreement has been entered into. Under a Data Use Agreement, only a statutorily defined "limited data set" can be shared; most PHI identifiers must be removed (e.g. names, addresses, etc.) and certain date information can be retained. The limited scope of use must be defined.

In addition to data use arrangements, institutions may use their own data sharing agreements. Similarly, they may need to comply with or negotiate the other party's form of agreements.

Entities must comply with GDPR requirements when the GDPR applies to the data subject.

Compliance with state privacy law may be required, including when biometric data is regulated personally identifiable information (as under Illinois state law).

4.3 Which key regulatory requirements apply?

The key regulatory requirements which apply are as follows:
- HIPAA/ HITECH as discussed above.
- The Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) protects the privacy of student educational records and requires consent for disclosure of information except for "directory information" (names, address, etc.).
- The GDPR.
- The CCPA.
- The California Confidentiality of Medical Information Act (CMIA) and other state laws may apply. The CMIA provides protection for an individual's medical record in paper or in electronic format from unauthorised disclosure.

4.4 Do the regulations define the scope of data use?

HIPAA/HITECH and FERPA define the scope of regulatory data use and the scope of exceptions to obligations of nondisclosure. See question 4.2.

4.5 What are the key contractual considerations?

The key contractual considerations are as follows:
- Whether a Business Associate Agreement is required.
- Whether a data processing agreement is required for personal information not subject to HIPAA.
- The time and scope of notification for data breaches and obligations to pay or reimburse fines, the costs of notices to data subjects required by state law, and the expenses of investigations.
- Rules on return or destruction of data.
- Injunctive relief, including specific performance.
- Whether data is provided "as is" or with warranty or assurances.
- The scope of representations, warranties and covenants, the scope indemnities for data breaches and breaches under contractual obligations and under Business Associate Agreement obligations, the scope of exceptions, and negotiating limitations of liability to the extent permitted by applicable law.
- Immediate termination rights for statutory violations.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Sharing personal information (including PHI) between organisations implicates regulatory requirements including obligations with respect to confidentiality and privacy.

Different parties to a data sharing arrangement may have different regulatory status, resulting in the need to structure agreements to address regulatory obligations and risks. Moreover, both parties may have liability if one party uses the data in contravention of statutes.

Both the covered entity and its business associate have direct liability for breaches.

From a technical point of view, the parties should consider the use of encryption to protect against unauthorised access. Companies as business associates must require their subcontractors to meet the obligations imposed on them.

5.2 How do such considerations change depending on the nature of the entities involved?

The considerations change as described in questions 4.2 and 5.1.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The key regulatory requirements discussed in section 4 are applicable to the sharing of personal information in the digital health context.

6 Intellectual Property

6.1 What is the scope of patent protection?

As relevant to digital health, US patent law can provide a greater scope of protection for software-based inventions than other jurisdictions. Novelty and non-obviousness are required for patentability, and the subject matter of the invention must be patent-eligible, which is the subject of evolving law in the US.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

The term of patent protection (with certain exceptions) is 20 years from the date of filing the application, assuming periodic maintenance fees are paid in a timely manner. A patent is not strictly speaking a monopoly because it is a right to exclude other parties from practising the patented invention, rather than the grant of a right to make, use or sell a product based on an invention free of claims of infringement of another patent which may apply to part of the product. Patent rights are enforced in federal and not state courts. There is no innocent defence to patent infringement.

6.2 What is the scope of copyright protection?

In the digital health context, copyright protects software as a work of authorship, and databases as compilations, provided there is sufficient originality in the structure, sequence and organisation of the database to meet the originality requirement. While copyrights arise automatically, the US has a procedure for copyright registration. Registration is a prerequisite for commencing an infringement action. It provides certain benefits, such as eligibility for "statutory damages", which are monetary amounts set forth in the Copyright Act, and can overcome the common difficulty of establishing the monetary value damages given the nature of copyright infringement. Registration also allows for the recovery of the attorney's fees in litigation. Registration within five years of publication establishes *prima facie* evidence of the validity of the copyright and facts stated in the copyright registration certificate, which identifies the owner of the copyright. This effectively shifts the burden of proof of non-infringement to the alleged infringer, which is beneficial to the owner when injunctive relief is sought. Registration requires the submission of a "registration deposit" copy of software and databases that meet the requirements under the Act. The US "work made for hire" rule vests ownership of the copyright in the employer for works created by an employee within the scope of his or her duties. However, the second branch of the "work made for hire" rule applies to subcontractors and other non-employees and automatically vests ownership in the retaining party only if the work of authorship fits within one of nine statutory categories, which are often difficult to apply to software. Accordingly, best practice is to obtain an assignment from a non-employee. The "work made for hire" rule does not apply to patent or trade secret rights. The term of copyright protection is the life of the author plus 70 years, unless the work had been created as a work made for hire, in which case the term is the shorter of 120 years after creation or 95 years after publication.

6.3 What is the scope of trade secret protection?

Trade secret protection applies to information that is not generally known to the public and confers economic benefit on its owner where the owner maintains it in secrecy. Disclosure under nondisclosure agreements can maintain the required secrecy. Unlike copyrights and patents, trade secrets have no fixed term and can theoretically be protected in perpetuity. Trade secret protection ends when the trade secret is no longer maintained in confidence.

6.4 What are the typical results on academic technology transfer rules?

Academic institutions typically have IP policies requiring that they own IP developed with their resources/funding, and then provide royalty sharing rules among the institution, applicable departments, and the professor/researcher.

Institutions often license the technology to companies in exchange for equity and/or royalties. Revenue generated often funds the research lab.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

The FDA defines SaMD using the definition of the International Medical Device Regulators Forum, which is "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device". In almost all cases, SaMD is copyrightable and trade secret subject matter. It may be eligible for patent protection, if, for example, the technology uses monitoring or sensor hardware or otherwise is characterised to turn a computing device into a specialised medical treatment device (e.g. virtual reality and AI), then a utility patent might be supported by system, method and/or device claims applicable to the SaMD technology. Specific screen interfaces or other visual electronic tools generated by the SaMD might also support design patents.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The prevalence of joint development agreements in healthcare technology and the collaborative efforts common to multi-disciplinary projects create potential unanticipated adverse business results under US IP laws. Reflexively defaulting to joint ownership for joint developments, while seemingly a fair business accommodation, in fact provides one joint owner under US default statutory patent rules with the right to contribute the other party's work product as free R&D to another venture without the permission or control of, or remuneration to, the other party. Moreover, joint ownership may not apply in an unambiguous way because copyrightable authorship is different from patentable inventorship. The better approach is to allocate ownership and licence rights by contract, especially when multiple parties bringing different capabilities are involved.

7.2 What considerations apply in agreements between health care and non-health care companies?

The nature of the transaction and how it fits in the applicable regulatory frameworks is an important part of the due diligence and advance work, as well as in structuring the agreement. For example, will the non-healthcare company be classified as a business associate? Due diligence should be conducted with respect to data rights and whether encumbrances will undermine business goals. Many US healthcare systems are faith-based or are non-profit institutions with policies and codes of conduct with which commercial entities need to become familiar as part of their due diligence. Academic medical centres have IP policies and procedures which create distinctive business arrangements. This emphasises the importance of giving careful thought to structuring IP rights. Non-healthcare companies selling technology to hospitals may need to factor in the need to "sell" the technology to one hospital department at a time in the hospital.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning uses datasets to train and improve the utility of algorithms. Machine learning has promising applications in diagnostic, decision-support, treatment monitoring, and intelligent automation. Its use in digital health includes the following: (i) analysis medical images to diagnose breast cancer and to otherwise identify abnormalities for clinicians to review in order to make diagnoses when those abnormalities would be hard to detect without the pattern recognition powers of machine learning; (ii) conducting statistical analysis of the efficacy of medications; and (iii) using natural language processing (NLP) to "mine" digital transcriptions of clinic notes, and using NLP to generate the digital transcription from voice recordings. In this regard, machine language-enhanced NLP may become an advanced interface for both the input and output of information between human beings and medical computer systems. AI-enabled chat-bots are providing "customer service" for family members of patients, and have the potential to gather meaningful medical information from patients to provide to physicians. AI and machine learning are being used to improve backroom hospital operations.

8.2 How is training data licensed?

Datasets in the form of copyright compilations can be licensed as an intellectual property right. The data can also be licensed by contract without absolute determination of the nature of the data property right. Datasets created for a purpose outside of healthcare can be licensed and repurposed to provide baseline training algorithms.

8.3 Who owns the intellectual property that is developed/improved by machine learning without active human involvement?

This is an open question under US intellectual property law. Currently, patent and copyright ownership are granted only to human inventors and authors. The Compendium of US Copyright Office Practice provides that works produced by a machine without creative input or intervention from a human do not have authorship to establish copyright. 35 U.S.C. § 100(f) of the US Patent Act similarly states: "The term 'inventor' means the individual or, if a joint invention, the individuals collectively who invented or discovered the subject matter of the invention." However, the US Patent and Trademark Office issued notices for public comment seeking guidance as to how AI and machine learning patent, copyright and trademark rights should be handled for purposes of ownership and registration. As of this publication, no final rules or comments have been promulgated. A related question is who can own the learnings that are derived from machine learning.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The commercial considerations that apply are as follows:

- The type of data:
  - Personally identifiable or other protected health information.
  - Fully de-identified health information in accordance with HIPAA.
  - Aggregated/anonymised personal information.
  - Non-regulated other data.
- The purpose of the data use:
  - Patient care and diagnosis.
  - To provide healthcare operations support to a covered entity (e.g. a hospital).
  - To improve the AI/machine learning vendor's products and services.
- The time period the vendor can retain the data:
  - A short period while processing for a specific user.
  - Use in an ongoing contractual relationship.
  - In perpetuity, including use by the vendor for its purposes.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

The theories of liability that apply are as follows:

- Negligence and law of torts.
- Breach of contract.
- Product defects under product liability theories.
- Regulatory violations.
- Violation of consumer protection laws.
- Discrimination based on biased algorithms.

9.2 What are the cross-border considerations?

Personal injury occurring in the US will generally be governed by US law. Delivery of healthcare through remote means has an unclear status and the contracts involved are likely to provide a basis for determining the applicable law. Arbitration can bring more certainty.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

The key issues in cloud-based services are as follows:

- Data controls, security and privacy, including:
  - HIPAA compliant cloud-hosting (at additional cost).
  - Security and control certifications and audit reports.
  - Audit rights for regulators.
  - Geolocation of the data, including a local (edge computing) data centre near the applicable health system, a national or regional US data centre, back-up and disaster recovery location.
  - Limited or unlimited liability.
- Data rights, including re-use or de-identification.
- Service levels, including availability and response times.
- Transition and migration rights.
- Termination rights.
- Risk allocation and liability, including with respect to medical decisions and care.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

The key issues that non-healthcare companies should consider are as follows:

- Separate policies, practices and infrastructure to support compliance with healthcare related laws and regulations which make transactions different from those in other industries.
- The time and investment to commercialise products and services and whether customers or investors require pilot programs. The revenue and monetisation model needs to be carefully considered, including with respect to patients, providers, hospitals, health systems, group purchasing organisations, self-insured company payors, insurance companies, and government reimbursement programmes.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

The key issues that venture capital and private equity firms should consider are as follows:

- Conducting healthcare regulatory and other due diligence and using healthcare regulatory counsel.
- The issues and factors in question 10.2, including with respect to investment and commercialisation time horizons, cash flow, and revenue and monetisation models.
- Legal exposure or uncertainty if the technology exceeds the current state of regulation and government programmes.
- Conducting IP due diligence to determine the offensive and defence competitive advantages the venture has from the existing IP portfolio and risk of infringement.

Additional Co-Authors

The additional co-authors of this chapter are Lidia Niecko-Najjum, Mark Petry and Jason Putman Gordon.

Lidia Niecko-Najjum is a U.S. healthcare regulatory attorney. With over 10 years of cumulative experience in nursing, policy, and law, Lidia's practice focuses on healthcare regulatory, coverage and payment, compliance, transaction, and policy matters, with special focus on digital health and HIPAA and health information privacy and security. Lidia's representative clients include digital health companies, academic medical centres, health systems, acute surgical centres and long-term care facilities.
Tel: +1 202 626 8396 / Email: lnieckonajjum@polsinelli.com

Mark Petry provides strategic counsel on digital health matters with respect to intellectual property, research and development, commercialisation, data analysis and processing, clinical and business processing, and/or the financing or monetisation of digital health assets and technologies. He represents emerging and established companies ranging from technology start-ups to large internationally recognised health systems and medical device providers, who desire to develop, buy or sell, license, incubate, pilot, or adopt new innovative digital health technologies and/or transform their business and operations. He has represented numerous companies in developing and applying artificial intelligence and machine learning technologies, cloud and other big-data solutions, and remote care or monitoring programs or devices. He also understands and knows how to address the concerns and dynamics between various industry participants, including healthcare providers, device and data companies, and insurers and other payors.
Tel: +1 202 772 8474 / Email: mpetry@polsinelli.com

Jason Putman Gordon is a results-oriented corporate attorney practising in the Venture Capital and Emerging Growth Companies group in Polsinelli's San Francisco office. Jason has a passion for working with experienced entrepreneurs and executives to make their vision a reality. In his practice, he regularly represents companies throughout their life cycle in matters related to venture capital financing, strategic corporate relationships, corporate formation, complex mergers and acquisitions, sales, and divestitures. With industry focuses on consumer goods and technology, because of his broad skill set and deep network, Jason regularly works in wide array of verticals including artificial intelligence, virtual reality, augmented reality, video games, software, hardware, life sciences, the Internet of Things and agricultural technology. Jason works with companies based locally, elsewhere in the U.S. and internationally.
Tel: +1 415 248 2154 / Email: jgordon@polsinelli.com

© Published and reproduced with kind permission by Global Legal Group Ltd, London

William A. Tanenbaum is the Practice Co-Chair of Polsinelli's Health Care Technology & Innovation Group, which is the second largest of its type according to the American Health Lawyers Association. Bill is the past President of the International Technology Law Association and was named by his peers as "Lawyer of the Year" in IT in New York in research by *US News & World Report*. He is the only lawyer ranked in Technology in the US and Global editions of *Chambers* whose practice focuses on healthcare. *Who's Who Legal* says he is a "well-known and highly respected practitioner" who has "expertise in technology transactions that puts him at the very top of the market", and that he is a "go to expert" on "the management and protection of data". *Chambers* finds that he "brings extremely high integrity, a deep intellect, fearlessness and a practical, real-world mindset to every problem".

Polsinelli PC
600 Third Avenue, 42nd Floor
New York, NY 10016
USA

Tel: +1 212 413 2840
Email: wtanenbaum@polsinelli.com
URL: www.polsinelli.com

Michael Gaba, Vice Chair of Polsinelli's FDA Practice Group, represents life science companies before the U.S. Food and Drug Administration on a range of pre-market and post-market regulatory issues, with an emphasis for more than 20 years on medical device manufacturers and more recently software developers looking to make informed business judgments, factoring in the pros and cons of being regulated as a medical device. Michael counsels a host of clients, from start-ups to mature medical device manufacturers, on labelling and pre-market strategies, the FDA's software as medical device pre-certification pilot program, product approvals, and post-market compliance.

Polsinelli PC
1401 Eye ("I") Street, N.W.
Washington, D.C., 20005
USA

Tel: +1 202 772 8496
Email: mpetry@polsinelli.com
URL: www.polsinelli.com

Eric J. Hanson is a registered patent attorney and intellectual property shareholder at the Polsinelli law firm. Eric has worked in all aspects of domestic and international intellectual property law for over 20 years. His extensive experience includes protection, risk assessment and commercialisation of cutting-edge technologies, including medical devices, personalised medicine, hardware/software enhancements and functionality, communications, artificial intelligence, data processing, internet & business methods, 3D printing, life sciences, and biotechnology.

Polsinelli PC
1201 West Peachtree Street N.W.
Atlanta, Georgia 20209
USA

Tel: +1 404 253 6272
Email: ehanson@polsinelli.com
URL: www.polsinelli.com

Erica Beacom provides counsel on digital health matters related to healthcare entity research and development, privacy data analysis and processing, clinical and business processing, and development of medical devices, including Software as a Medical Devices ("SaMD"). She represents a range of companies including healthcare systems, medical device providers, startups, and pharmaceutical-based entities involved in the adoption and implementation of innovative digital health technologies. She has represented numerous companies entering the SaMD regulatory space with a focus on innovative early identification treatment programmes reliant upon personal health information and medical data. She understands the dynamic between industry participants, including the FDA, healthcare providers, device and data companies, and insurers (including both private and federal healthcare programmes).

Polsinelli PC
1401 Eye ("I") Street, N.W.
Washington, D.C., 20005
USA

Tel: +1 202 772 1487
Email: ebeacom@polsinelli.com
URL: www.polsinelli.com

Polsinelli PC is a full-service AmLaw 100 firm with 900 lawyers in 21 cities in the United States. Its Health Care Department is one of the largest in the nation and its Health Care Technology & Innovation Group is the second-largest healthcare IT practice, both according to the American Health Lawyers Association. *US News & World Report* recognised the Health Care Department as a National Tier One practice for the last seven years and ranked Polsinelli as the "Law Firm of the Year" in healthcare. The firm also has a healthcare consulting firm, Polsinelli Health Care Solutions. The Technology Transaction & Data Privacy Group, which provides cross-disciplinary services with the Health Department, also received a National Tier One ranking. BTI Consulting ranks the Health Department in the top 3% in client relations and Polsinelli as one of the Top 30 firms in the US for client service.

www.polsinelli.com

POLSINELLI

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Venezuela


Victoria Montero


Carlos García Soto


Joaquín Nuñez

LEĜA Abogados
Hoet Pelaez Castillo & Duque

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no general definition of digital health in Venezuela. However, there is a definition of telemedicine which is included in the Telehealth Law, which came in effect in 2014.

This law had the purpose of implementing a Telehealth Network within the public health system. This purpose has still not been fulfilled as the government never created such a network. However, it is the only piece of legislation that contains a close concept to that of digital health.

The above-mentioned law defines telemedicine as "*the combined use of information and communication technology through free software for the remote provision of healthcare services by health workers, for the exchange of reliable information in the diagnosis, treatment and prevention of diseases, research, evaluation and medical education with the purpose of improving the health of individuals, families and communities*".

1.2 What are the key emerging technologies in this area?

Venezuela has a small entrepreneurial sector focused on the development of health technologies. The most relevant developments are concentrated in building software to keep digital health records, applications for the storage of health images in the cloud and software that facilitates the internal management of patients within health centers.

However, the most common use of technology has been in the area of telemedicine. There are several platforms that allow patients to have online medical consultations with Venezuelan doctors. These platforms have been developed by private clinics or independent health professionals. Also, in most cases their creation has been directed to attend Venezuelan migrants' medical needs abroad.

1.3 What are the core legal issues in health care IT?

We consider that the most challenging legal issue regarding healthcare IT is the lack of regulation on matters related to data protection and data privacy.

Although healthcare professionals are governed by several laws that regulate issues such as the confidentiality of the information shared by the patient, our current legal framework does not develop in detail relevant issues such as the responsibility that IT providers have in the protection of the data shared through these technologies.

Also, our current legal framework does not impose any standards regarding the type of safety infrastructure that providers of healthcare IT services must have in order to avoid unauthorised access to the information, or what the consequences are if a safety breach occurs and the patient's data is available to third parties.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The core healthcare regulatory scheme is the one contained in the Organic Health Law, some of which is further developed in the Law of the Practice of Medicine.

The Organic Health Law regulates the rights of patients, establishes legal principles on the quality of the health services for public and private healthcare providers, and regulates the type of injunctions that the public administration can impose to healthcare providers whose actions have endangered the population's health.

On the other hand, the Law of the Practice of Medicine develops in detail the duties of doctors in relation to patients in special circumstances, such as epidemic outbreaks, events in which the patient does not want to continue with the recommended medical treatment, and the standard of conduct when the doctor deals with emergency cases or when the patient is unconscious.

The Law of the Practice of Medicine also develops what constitutes medical secrecy, what its scope is, and what the exceptions are under which the communication of medical information is not considered a violation of the medical secrecy duty.

Also, we consider that it is worth mentioning the regulatory scheme contained in the Organic Law of Just Prices. This law regulates the sale of all types of services and goods, including healthcare services. Although its main purpose was to establish rules that would regulate the prices of services and goods, it also includes a set of rights that consumers have and a list of applicable sanctions to service providers that violate those rights, including healthcare providers.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

2.2 What other regulatory schemes apply to digital health and health care IT?

Digital health could imply the use of wearable devices or monitoring sensors that might be used by healthcare professionals to diagnose or treat a patient. Under Venezuelan law, these types of tools are considered medical devices.

The regulatory scheme applicable to such products is comprised mainly by Resolution No. 55 and Resolution No. 164 issued by the Ministry of Health. These resolutions define what a medical device is, the types of medical devices, the procedure for requesting marketing authorisation for such products, and other issues related to that authorisation.

2.3 What regulatory schemes apply to consumer devices in particular?

Consumer devices are regulated by the Organic Law of Just Prices, mentioned in question 2.1 above. This law establishes rights that consumers have when purchasing a good or service. Such rights include receiving quality goods, receiving truthful information about the product and receiving compensation for damages caused by the use of the products, among others.

Also, this law establishes that any goods that have mechanical or electrical systems must have a manufacturer or seller's warranty against any fabrication flaw or malfunctioning.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The main regulatory authority is the Ministry of Health that, through the Sanitary Comptroller, enforces the rules contained in the Health Organic Law and Law for the Practice of Medicine and it has jurisdiction to impose administrative sanctions on healthcare professionals and healthcare institutions that violate the norms contained in such laws.

Also, the Sanitary Comptroller also enforces the regulatory scheme related to medical devices and has jurisdiction to audit and to impose administrative sanctions on manufacturers or importers that violate the applicable norms or endanger the population's health.

On the other hand, the National Superintendence for the Defense of the Socioeconomic Rights (SUNDEE for its Spanish acronym) is the agency that enforces the Organic Law of Just Prices. The SUNDEE has jurisdiction to carry out auditing and sanctioning procedures against companies that violate the law, including manufacturers or importers of consumer devices.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

Digital health and healthcare IT are new sectors with little penetration in the Venezuelan market. Hence, currently there are no known enforcement actions carried out by the authorities.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

There are no express regulations on the use of software as a medical device. The language in Resolution No. 164 issued by the Ministry of Health that contains the definition of medical device, establishes that a "system" might be classified as such a product. However, the meaning of the word is not precise and it is not clear whether the health authorities would consider software a system that is used as a medical device.

We have no knowledge of software that has been classified and registered as a medical device in Venezuela.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  As mentioned in question 1.1 above, Venezuela has a Telehealth Law, which came into effect in 2014. The purpose of the law was to implement a Telehealth Network within the public health system.
  The law established some obligations for providers of telehealth services within the Network. Such obligations included the acquiring patient's authorisation before the doctor performs the medical consultation and the duty to not disclose the patient's data. Also included is the obligation for the Telehealth Network to have technological protective measures that guarantee the confidentiality and integrity of the information. The applicability of these rules to private providers only extend to those that render their services within the Telehealth Network.
  However, as previously discussed, this law was never implemented, as the Network was never created. The enforcing agency was also never created. Instead, we have seen the surge of private initiatives in this realm as mentioned in question 1.2. above, that might apply some of the principles contained in the law, but are not directly regulated by it.
- **Robotics**
  Venezuela does not have a specific legal framework applicable to robotics. Hence, tools developed with robotics technology are most likely considered medical devices.
  For several years now, healthcare professionals in Venezuela have used robotic devices to perform surgeries, but to the best of our understanding, those devices are not self-controlled and are managed by the doctors performing the procedures.
- **Wearables**
  The core issue with wearables is whether they are classified as medical devices or not. The answer will depend on the claims that the importer or manufacturer makes.
  In the case of the manufacturer claiming that the product is intended for recreational and wellness purposes and that it must not be sued in a medical setting for the diagnosis or treatment of a diseases, the products will be considered as any other consumer device regulated by the general provisions of the Organic Law of Just Prices, discussed in question 2.3 above.
  Conversely, if the manufacturer or importer claims that the wearable can be used by a physician to diagnose or treat a disease, then it will be classified as a medical device. This will trigger the obligation to request marketing authorisation and comply with rules on manufacturing best practices.
- **Virtual Assistants (e.g. Alexa)**
  Venezuela does not have specific regulations on virtual assistants for use in health settings. As with wearables, the main issue would be if they can be considered as medical devices or just as consumer products.
  The definition of medical device in our legislation includes "systems" that can treat or diagnose a disease which in theory can include a system such as a virtual assistant. However, in our opinion, it is unlikely that such product can achieve the safety and efficacy standards to be authorised as a medical device.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Hence, the use of a virtual assistant for medical use in Venezuela would probably not be permitted. In our view, these products could, in the best scenario, make wellness and recreational claims.

- **Mobile Apps**
  As with wearables, the nature of the technology would determine its use in the realm of digital health. For instance, apps that use algorithms to diagnose a disease based on the symptoms recorded by the user might be considered a medical device, according to local regulations. However, as with virtual assistants, complying with safety and efficacy standards might be challenging for this type of technology.
  On the other hand, if an app is used to contact a health professional to have a medical consultation, then this might be considered as a telemedicine application, which, as discussed above, is not regulated and the only limits would be those set out in the Law of the Practice of Medicine.
- **Software as a Medical Device**
  Please see our comments in question 2.6 above.
- **AI-as-a-Service**
  Venezuela does not have specific regulation on AI as a healthcare service provider. Again, we consider that the core issue would be the nature of the technology: a medical device or a simple consumer product. And this will depend on how safely and effectively the technology can diagnose and treat a disease.
- **IoT and Connected Devices**
  There are no regulations on the use of IoT and connected devices in a health setting. The legal challenges will be similar to those discussed above for AI-as-a-Service.
- **Natural Language Processing**
  There are no regulations on the use of Natural Language Processing for medical purposes. As this technology is used in a broad range of devices, it would be necessary to analyse the exact application thereof. However, we consider the capacity to safely and efficiently diagnose a disease or a health condition would determine its use as a medical tool in the provision of healthcare services.

3.2 What are the key issues for digital platform providers?

Digital platform providers in the health sector are not regulated by any health regulatory scheme. Hence, the main issues, such as liability in case of malfunctioning of the platform on which the technology relies, must be regulated by the agreements entered into between such platforms and the provider of the service.

Also, as we will discuss in section 4 below, Venezuela does not have a sophisticated regulatory framework on data privacy and data protection. Hence, those issues must be clearly regulated in the agreements entered into between the digital platform and the service provider.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Venezuela does not have a specific law that regulates data privacy and data protection matters. Instead, there is a constitutional right to access one's own personal data that is stored in either public or private records. The owner of such data is also entitled to know about the use and purpose and to request the update, rectification or destruction of the data he or she considers to be harmful to his or her interest.

This constitutional right was interpreted by the binding Decision No. 1318 issued by the Supreme Tribunal, which enumerated a set of principles that must be complied with in the collection of personal data. The key principles are: (i) request consent from the subject to collect the data; (ii) inform the subject of the purpose for the collection of data and comply with such purpose in using the data; (iii) do not keep the collected data beyond the fulfilment of the data collector's purpose for the collection of the data; (iv) inform the subjects of the procedures on how to retrieve his or her data; and (v) guarantee that the data will not be transferred to unauthorised third parties. The Tribunal also included the guarantee not to transfer data to international jurisdictions that do not offer minimum standards of data protection, although the Tribunal recognises that issues such as the nature of the data and the consent of the subject must be taken into account when transferring the data to less regulated jurisdictions.

On the other hand, if the person collecting the data is a health professional in the exercise of his or her profession (e.g. in a telemedicine consultation), then the use of personal data is also governed by the Organic Health Law and the Law of Practice of Medicine. The Organic Law determines that every patient has the right to a confidential treatment of his or her medical information. On the other hand, the Law of the Practice of Medicine establishes the obligation to guard the medical secret. The scope of what constitutes a medical secret is very broad and refers to all information that the physician learns while practising his or her profession. Other medical staff might also be obliged to keep medical secrecy, and this includes medical students, paramedics and other healthcare professionals. In general, a healthcare professional would require the patient's authorisation to disclose the medical information to a third party.

4.2 How do such considerations change depending on the nature of the entities involved?

As discussed in question 4.1 above, the only difference would be if the person collecting the data were a health professional practising his or her profession. In such case there would be a higher standard of care in the use of the medical information. The general data privacy rules would apply to any kind of entity involved.

4.3 Which key regulatory requirements apply?

As discussed in question 4.1 above, the main regulatory requirements for the use of personal data are: (i) to request consent; (ii) to inform the subject of the purpose for the collection of data and comply with such purpose; (iii) to not keep the collected data beyond the fulfilment of the data collector's purpose; (iv) to inform the subjects of the procedures on how to retrieve his or her data; and (v) to guarantee that the data will not be transferred to unauthorised third parties.

These are just basic principles developed by Decision No. 1318; however, there are no specific guidelines on how to comply with them, especially in terms of consent and what constitutes valid authorisation.

4.4 Do the regulations define the scope of data use?

No, local regulations do not define the scope of data use. The data collector is required to inform the owner of such data and

© Published and reproduced with kind permission by Global Legal Group Ltd, London

the purpose for which it will be used. But the scope for how data can be used is not established in the legal framework.

4.5 What are the key contractual considerations?

As discussed in questions 4.1 and 4.3, contractual regulations between the collector of the data and the data owner must clearly cover and comply with the principles set forth in Decision No. 1318.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Please see questions 4.1 and 4.3 above.

5.2 How do such considerations change depending on the nature of the entities involved?

The only difference would be if the person collecting and sharing the data is a healthcare professional practising his or her profession. In such case there would be higher standard of care for the sharing of the medical information.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please see questions 4.1, 4.3 and 4.5 above.

6 Intellectual Property

6.1 What is the scope of patent protection?

Venezuelan National Patents (invention, industrial models and industrial drawings) have a duration of 10 years from the date the application is granted, subject to the payment of annuities.

The scope of protection conferred by a patent is determined by the content of the claims. The description and drawings shall be used to interpret the claims.

The patent shall confer on its owner the right to prevent third parties who do not have his or her consent to engage in any of the following acts:

- where the patent claims a product: (a) manufacture the product; (b) offer the product for sale, sell or use it, or import it for any of those purposes; and
- where the patent claims a process: (a) use the process; or (b) carry out any act in relation to a product obtained directly by means of the process.

6.2 What is the scope of copyright protection?

The Law on Copyright currently in force establishes that the author's economic rights shall be automatically and fully transferred to the natural or legal persons that produce or publish the work for the entire duration of the right, unless otherwise stipulated.

Similarly, such law stipulates that the economic rights of the author(s) of works created under employment or commissioned are to be definitively transferred to the employer or commissioning party, unless established otherwise.

Also, the law determines that the right lasts the lifetime (of the author) and shall expire 60 years from the 1 January of the year after his/her demise. This is also applicable for undisclosed works.

6.3 What is the scope of trade secret protection?

In Venezuela, trade secrets are not explicitly contemplated under intellectual property regulations.

Thus, Venezuela applies the provisions of the Paris Convention and the Trade-Related Aspects of Intellectual Property Rights Treaty (TRIPs Agreement) on unfair competition, as well as the provisions established in the legal framework of Antitrust Law.

Even though the TRIPs Agreement and Paris Convention do not define what information is eligible for being classified as a trade secret, they do establish the conditions for its protection, which are: (i) that it is not easily accessible; (ii) it has a commercial value; and (iii) that reasonable measures to protect it have been taken.

The concept of "keeping the secret" exists in Venezuelan criminal legislation and also in civil legislation, as a not-to-do obligation infringement.

Thus, making an unauthorised disclosure of a trade secret is considered a violation of civil law and grants the right to compensation for damages.

6.4 What are the typical results on academic technology transfer rules?

Typical results on this matter consist in data and information that can be used for different purposes in digital health. The technology transfer rules can be established privately by the parties, including the scope of its use and possible dissemination.

In addition, the Law of Science, Technology and Innovation, which deals with the technology transfer rules, states: "The Ministry of Science and Technology shall promote, with the competent bodies and members of the National System of Science, Technology and Innovation, policies and programs aimed at defining the ownership and protection of intellectual creations resulting from scientific and technological activity, all in accordance with the regulations governing the matter."

Accordingly, the Ministry of Science and Technology can establish policies and regulations for this purpose, aiming to promote technology and innovation in our country.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

In Venezuela, software can be protected as a trade secret or as copyrighted material. The exclusive right of exploitation of software as a medical device is regulated by the Venezuelan Copyright Law. The author enjoys the exclusive right to exploit his work in whatever manner he sees fit and to derive profit therefrom.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The parties can establish the terms for collaborative improvements in protected intellectual property works. If no provisions are set or established for this purpose, depending on the

© Published and reproduced with kind permission by Global Legal Group Ltd, London

type of intellectual property involved, specific rules may apply. The general rule is that the authors are entitled in the same percentage to their collaboration, which is directly related to work and improvements, unless otherwise stated.

7.2 What considerations apply in agreements between health care and non-health care companies?

Applicable considerations will depend on the purpose of the commercial agreement. However, in general, commercial agreements between healthcare and non-healthcare companies must guarantee the rights of the patients impacted by such agreements, especially the protection of the patient's data and right to confidentiality which is an important aspect of health technologies.

In addition, although data security infrastructure is not mandated in local norms, companies treating patients' personal data should ensure these measures are taken in all their agreements to avoid any security breaches and to regulate responsibilities and procedures to diminish risks in this area.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

To the best of our knowledge there are no relevant or specific cases in which AI and machine learning are being used in the field of digital health locally.

8.2 How is training data licensed?

This data can be currently licensed by means of private contracts, in accordance with the provisions established by the parties and within the scope of data regulations discussed in sections 4 and 5 above.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

In Venezuela there are no laws specifically regulating ownership of intellectual property rights when it comes to algorithms enhanced by machine learning without human participation. However, it is likely that the person or company that owns the machine would be considered as the rightful owner of the improved algorithms.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The most important issue in licensing training data is that it complies with the data privacy rules established in Venezuelan legislation.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

There are no specific theories of liability applicable to adverse outcomes in digital health. In general, tort law provides private plaintiffs with a right of action to claim damages due to harm or loss caused, against a person or company who has caused such loss or harm. This includes healthcare professionals.

On the other hand, if the digital health product is classified as a medical device, the holder of the marketing authorisation might be subject to administrative sanctions in case the adverse outcome was due to the breach of the health regulations applicable to this type of product. Consumer goods are also subject to administrative sanctions under the Organic Law of Just Prices. Also, healthcare professionals are subject to administrative sanctions according to the Organic Health Law and the Law for the Practice of Medicine.

Criminal actions are also available against manufacturers or importers of products, as well as against healthcare professionals if the adverse outcomes amount to a felony or crime established in the Penal Code.

9.2 What cross-border considerations are there?

The Law of Private International Law determines that local courts have jurisdiction in actions against foreign entities with no residence in Venezuela and when those actions have an economic component, such as the payment of damages or the circumstances that caused the potential payment occurred in the country, e.g. if the harm or loss caused by the malfunctioning of a digital health technology occurred in Venezuela.

However, even if the Venezuelan tribunals have jurisdiction, the enforcement of a foreign court judgment will depend on whether the jurisdiction of the defendant recognises such foreign judgment under its laws.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

There are no additional issues, except the ones related to the compliance of the data privacy rules and requirements. Also, although it is not a legal requirement, companies should have technological safeguards that would reduce the risk of any breach of the data stored in the cloud to protect patient's confidential information.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

In our opinion, non-healthcare companies must carefully analyse whether the products that they will sell can be used effectively and safely in a medical setting. They must consider whether the claims they make about the products would cause the classification of the technology as a medical device and hence result in the compliance of strict regulations, including the licencing process.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

We consider that they must thoroughly analyse the nature of the products and their regulatory requirements and how the patient's data will be protected. They must also ensure that the intellectual property involved is properly protected under the local legal framework.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Victoria Montero joined LEĜA Abogados in 2013 as part of the corporate and M&A practice area. Victoria has extensive experience in the pharmaceutical sector and has been the leader of the M&A transactions that the firm has handled in the life sciences sector. She also has strong experience advising clients in the life sciences and healthcare industry in general contractual matters and regulatory issues. She also advises companies in the sectors of food, beverages, and agroindustry; oil and gas; banking and finance; and digital media and telecommunications. Victoria holds an LL.M. from Georgetown University Law Center (Washington, D.C.), 2018, and during her studies served as a research assistant to the O'Neill Institute of National and Global Health Law in Washington, D.C.

LEĜA Abogados
Av. Eugenio Mendoza. Urb. La Castellana
Torre La Castellana, Piso 7
1060-A, Caracas
Venezuela

Tel: +58 212 277 2240
Email: vmontero@lega.law
URL: www.lega.law

Carlos García Soto became a partner at LEĜA in 2019 after being a partner at Andrade, Weffe & García Abogados and Imery Urdaneta. Carlos has advised domestic and foreign companies in complex regulatory issues and has designed effective strategies for clients in highly regulated industries, including pharmaceuticals, healthcare and food and beverages. He has also successfully represented clients in administrative proceedings before various authorities, as well as before contentious-administrative courts on matters related to administrative acts and in relation with contracts entered with the state.
Carlos holds a Ph.D. from Universidad Complutense de Madrid and has been a visiting scholar in Columbia University (New York City, New York) and Universidad de Navarra (Pamplona, España). Carlos has authored many articles on administrative law matters and is the current editor of Universidad Monteávila's Law Journal, Derecho y Sociedad.

LEĜA Abogados
Av. Eugenio Mendoza. Urb. La Castellana
Torre La Castellana, Piso 7
1060-A, Caracas
Venezuela

Tel: +58 212 277 2211
Email: cgarciasoto@lega.law
URL: www.lega.law

Joaquín Nuñez is an attorney who graduated from the Universidad Catolica Andres Bello (Caracas, Venezuela), with an LL.M. in Intellectual Property Law obtained from The John Marshall Law School (Chicago, Illinois, USA) in 2008. He also obtained an MBA from the Golden Gate University (San Francisco, California, USA) in 2012.
Joaquín joined HPCD in 2012 and became senior partner in 2016. He worked for many years in a renowned law firm in the USA, where he gained a valuable international perspective. He started his professional career in 2004 and has worked in other well-known intellectual property firms in Venezuela.

Hoet Pelaez Castillo & Duque
Torre IASA, Piso 3
Av. Eugenio Mendoza
Plaza La Castellana
Caracas, 1060
Venezuela

Tel: +58 212 201 8601
Email: jnunez@hpcd.com
URL: www.hpcd.com

© Published and reproduced with kind permission by Global Legal Group Ltd, London

LEĜA is a leading law firm in the Venezuelan market and a benchmark in the international arena, with a modern approach to the practice of law. Our mission is to provide high-level legal services to clients, with a focus on delivering results in a profitable manner, while using the best technology. The firm has significant national and international reach through its offices in Caracas, Valencia, and Barquisimeto, and has representatives in London, Madrid, and Miami, in addition to many correspondents and professional networks worldwide.

As a firm, LEĜA has received many recognitions and awards. Their lawyers have more than 40 recognitions granted by the most important legal publications in the world, which have also certified the high quality of all the practice groups of the firm. With a strong international and business focus, LEĜA is the preferred firm of a large number of multinational clients in Venezuela.

www.lega.law

With over 75 years of experience, Hoet Pelaez Castillo & Duque (HPCD) is the leading IP firm in Venezuela and one of the most recognised with a strong international reach. We are a full practice IP law firm, characterised by always being at the forefront and innovating to provide personalised attention to meet the needs of our clients, becoming their allies in the development and protection of their Intellectual Property rights in Venezuela, Latin America and the Caribbean.

www.hpcd.com

ICLG.com

© Published and reproduced with kind permission by Global Legal Group Ltd, London

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group