International
Comparative
Legal Guides

Practical cross-border insights into digital health law

Digital Health 2022

Third Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

ICLG.com

ISBN 978-1-83918-172-6
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

Production Editor
Jane Simmons

Publisher
James Strode

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Digital Health 2022

Third Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

Introductory Chapters

Expert Analysis Chapters

Q&A Chapters

From the Publisher

Dear Reader,

Welcome to the third edition of *ICLG – Digital Health*, published by Global Legal Group.

This publication provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to digital health laws and regulations around the world, and is also available at www.iclg.com.

This year, two introductory chapters provide an overview of digital health, as well as the rise of digital therapeutics in the corresponding legal, regulatory and policy landscape.

In addition, two expert analysis chapters cover the global landscape of digital health and the balance between digital health and data protection in the context of COVID-19.

The question and answer chapters, which in this edition cover 20 jurisdictions, provide detailed answers to common questions raised by professionals dealing with digital health laws and regulations.

As always, this publication has been written by leading digital health lawyers and industry specialists, for whose invaluable contributions the editors and publishers are extremely grateful.

Global Legal Group would also like to extend special thanks to contributing editor Roger Kuan of Norton Rose Fulbright for his leadership, support and expertise in bringing this project to fruition.

James Strode
Publisher
Global Legal Group

ICLG.com

Introduction


Roger Kuan


David Wallace

Norton Rose Fulbright
Johnson & Johnson

What is Digital Health?

The rapid convergence of digital technologies with healthcare over the past five years (even prior to the COVID-19 pandemic) has transformed how healthcare is delivered to the masses. The promise of digital technologies continues to transform the healthcare delivery model from a traditional model based on a "one size fits all" practice of medicine that was characterised by a provider-centric approach with information silos, to a new model that is focused on patient-centric treatment personalisation with high data accessibility and utilisation. The result is a highly personalised healthcare system that is focused on data-driven healthcare solutions and individualised delivery of therapeutics and treatments to patients using information technologies (IT) that enable seamless integration and communication between patients, providers, payors, researchers and health information depositories. A November 2020 report by Precedence Research published on *GlobeNewsWire* indicates that the global digital health market is poised to grow at a compound annual growth rate (CAGR) of around 27.9% over the next seven years to reach approximately $833.44 billion by 2027.[1]

Traditional Healthcare Paradigm

"One size fits all" approach

Disease diagnosis and treatment have traditionally been based on efficacy validation models that neatly packaged patient populations into distinct buckets (often focused just on the disease state in question) that rarely allowed for differentiation between the individual constituents. This "one size fits all" approach did not enable true personalisation of patient diagnosis and treatment based on their innate individual characteristics (e.g., genome, epigenome, proteome, microbiome, metabolome, morphology, etc.) and exposome (e.g., lifestyle, environmental exposure, socio-economic status, etc.).

One main reason why the healthcare industry adhered to the "one size fits all" paradigm for so long was the lack of capable and affordable tools and methodologies that could accurately monitor and determine all aspects of an individual's innate characteristics and then utilise that data to precisely tailor treatments or infer clinical outcomes for an individual. Due to recent digital health advances and availability of large volumes of relevant data, many of those technical hurdles have been overcome. The cost of generating and processing data that is indicative of an individuals' uniqueness (e.g., whole genome sequencing, proteomic analysis, high resolution imaging, etc.) has recently come down to such an extent that it is readily accessible to the masses and recent advances in artificial intelligence (AI) (more specifically, machine learning (ML)) techniques have powered the analysis of large and complex datasets generated by these tools to make clinically relevant insights that can help guide the diagnosis and treatment of patients based on their individual uniqueness.

Provider-centric model

Until recently, healthcare services were delivered to patients primarily through a provider-centric model, whereby patients seeking medical attention were required to go to a medical practitioner, clinic or hospital to be diagnosed and/or treated for their condition. This approach was largely driven by the healthcare industry's slow adoption of new IT (e.g., Internet of Things (IoT), wireless video communication, text messaging, electronic medical record systems, etc.) and the lack of digital health tools (e.g., wireless diagnostic medical devices, wearables, mobile apps, etc.) that allow for remote patient diagnosis and monitoring.

In the last few years, the healthcare industry's adoption of new IT technologies and other digital health tools has accelerated significantly, ushering in a new patient-centric paradigm (e.g., telemedicine, virtual healthcare, etc.) whereby healthcare services are delivered remotely to patients (almost on-demand), regardless of where they are. When the COVID-19 pandemic took hold of the world, a measure of urgency was also added as the provider-centric approach to healthcare now included a component of danger that patients would be exposed COVID-19 if they visited their providers in person.

Siloing of health information and data

Data access and analytics is the fuel that drives digital health. Patient health information has traditionally been either stored as physical files at a provider site (e.g., doctor office, clinic, hospital, etc.) or in electronic health record management systems that are incompatible with one another. This resulted in health data being siloed where they were stored, which hindered the seamless communication and sharing of health data. This also prevented the use and aggregation of such data to power analytics tools (many of which are driven by AI/ML) that are used in a variety of different applications, including drug discovery, diagnostics, digital therapeutics, pre-surgical planning, and clinical decision support.

New Digital Technologies

A host of different digital technologies are helping to provide the infrastructure and know-how to drive the digital health revolution in healthcare.

Wireless connectivity and IoMT

Wireless/mobile devices (e.g., mobile phones, wearables, medical devices, mobile applications, etc.) allow patients to access their healthcare providers and resources from anywhere around the world with wireless or WiFi data connectivity. In turn, this also allows their healthcare providers to monitor their current health status and condition. This amalgamation of devices can all be connected to enterprise healthcare information systems using networking technologies to form an Internet of Medical Things (IoMT) that allow for uniform transfer of medical data over a secure network.

Big data analytics/storage

The voluminous quantity of medical data captured and transmitted through an IoMT is then stored and analysed using Big Data storage and analytics systems that manage, curate and process the data to generate predictive insights and/or visualise the data to aid analysts in quickly interpreting the data. A 2017 white paper from Stanford University School of Medicine estimates that 153 exabytes of healthcare data was generated in 2013, and that was projected to grow to 2,314 exabytes by the year 2020.[2] Analytics can be performed on the data using traditional statistical data analysis tools or more advanced AI/ML methodologies.

Enabling New Digital Health Solutions

The adoption of digital technologies in healthcare has given rise to a number of different categories of transformative digital health solutions.

Remote patient monitoring and delivery of care

Perhaps the most visible and impactful of the categories of digital health solutions are telemedicine/telehealth and virtual care. 2020 was a banner year for telehealth as the COVID-19 pandemic led to an exponential leap in the number of patient consults using telehealth platforms due to social distancing measures and to minimise exposure.

A 2020 report by Amwell found that before COVID-19, fewer than 1% of all physician visits in the U.S. were conducted via telehealth; in just over a month after the start of the pandemic, analysis of health claims data found that this number had increased to over 50%. Of those patients who used telehealth platforms, over 90% said that they planned to continue using those platforms post-COVID-19.[3] The digital technologies that enable telehealth are wireless/mobile devices and the applications that run on them.

Moving beyond virtual doctor's visits through telehealth platforms is the concept of virtual care, whereby healthcare providers remotely deliver the full range of health services to patients by remotely monitoring patient condition and vitals (remote patient monitoring) using IoMT connected wearables and wireless medical devices; and communicate with patients to provide treatment advice and answer their questions using wireless/mobile devices that enable live and secure video, audio and instant messaging communication. This next step in the evolution of telehealth will truly change the traditional provider-centric model of healthcare delivery to patients to a patient-centric model where the wide range of healthcare services can be delivered virtually on demand and remotely wherever the patient is located.

Big data analytics and AI/ML-powered healthcare solutions

- **Personalised/precision medicine**
  Personalised/precision medicine is another digital health solution that has recently gained traction. These are healthcare models that are powered by Big Data analytics and/or AI/ML to ensure that a patient's individual uniqueness (e.g., genome, microbiome, exposome, lifestyle, etc.) factors into prevention and the treatment (e.g., therapeutics, surgical procedures, etc.) of a disease condition that the patient is suffering from. An example of this would be companion diagnostic tests that are used to predict a patient's response to therapeutics based on whether they exhibit one or more biomarkers. Large quantities of patient records including measured data of one or more patient biomarkers, the therapeutic(s) the patient is taking and the patient's clinical outcome can be analysed using Big Data statistical software tools to determine the biomarker(s) associated with a particular clinical outcome when the patient is treated with a particular therapeutic; or be used to train AI/ML algorithms that can identify biomarker(s) of relevance and infer patient clinical outcomes when treated with a particular therapeutic.
- **AI/ML enabled Diagnostics**
  The application of advanced AI/ML algorithms and techniques to process healthcare data enables critical clinical insights that link previously unrelated data inputs (e.g., imaging features, genomic/proteomic/metabolomic/microbiome biomarkers, phenotypes, disease states, etc.) to disease conditions and progression. This has resulted in diagnostic tests that have a high degree of predictive accuracy for some previously difficult to diagnose health conditions such as dementia, depression, Alzheimer's, and also enabled more non-invasive methods to diagnose and monitor disease conditions (i.e., cancer) that previously required surgical biopsies or other more invasive techniques.
- **Intelligent drug design and discovery**
  The same data that is used to train AI/ML algorithms for personalised/precision medicine purposes can also be repurposed to train algorithms that can be used for intelligent drug design and clinical cohort selection applications that aid in the discovery and the clinical study of new or novel therapeutics and re-purposing of existing therapeutics.
  For example, an AI/ML algorithm trained to predict biological target response and toxicity can be used to design novel (i.e., non-naturally occurring) chemical structures that have strong binding characteristics to a biological target with correspondingly low chemical and/or systemic toxicity. This ability to design a therapeutic compound "backwards" from looking at desired attributes (e.g., binding strength, toxicity, etc.) and then custom designing a therapeutic compound with those attributes, instead of traditional drug discovery methods that screen millions of compounds for the desired attributes, is potentially game-changing. Not only does it hold the promise to shorten the initial drug target discovery process as it moves away from looking for the proverbial "needle in a haystack" to a "lock and key" approach, but it will likely lead to drugs that have greater efficacy and less side effects for larger groups of patients.
  Those novel chemical compounds can then be administered to clinical cohorts selected using AI/ML algorithms trained to choose the most suitable patients to enroll for clinical trials used to study the efficacy and toxicity of the compounds. Currently, it takes an average 10–15 years and

$1.5–2.0 billion to bring a new drug to market with approximately half of the time and investment consumed during the clinical trial phases of the drug development cycle. One of the main stumbling blocks in the drug development pipeline is the high failure rate of clinical trials. Less than one third of all Phase II compounds advance to Phase III. More than one third of all Phase III compounds fail to advance to approval. One of the primary factors causing a clinical trial to fail is clinical cohort selection that fails to enroll the most suitable patients to a clinical trial.[4] Minimising errors in clinical cohort selection can potentially shorten the clinical trial phase and reduce the risk of clinical trial failures that are not attributable to the drug being studied.

Digital hospital

Traditional hospital workflows can be highly inefficient because of disorganisation in patient treatment workflows and difficulties that clinicians have in readily accessing or utilising patient medical information. Through the use of digital medical information management tools, much of this inefficiency can be eliminated by ensuring less workflow downtime and gaps in the way that a patient is diagnosed and treated once he/she is admitted to a hospital and allowing patient medical information to be accessed anywhere within the hospital through a multitude of different means (e.g., workstation terminals, mobile devices, etc.) and from information stored externally from the hospital.

Digital Health Legal Issues

There are many important legal issues that apply to digital health. These issues can be broadly divided into two categories: intellectual property rights (IPRs); and regulatory compliance.

Intellectual Property Rights

With respect to IPRs, there are registrable IPRs (e.g., patents, copyrights, etc.) and unregistered IPRs (e.g., data rights, trade secrets, know-how, etc.).

Patents and copyrights

With respect to digital health and patents, the most burning issue is subject matter patentability (or what qualifies as patentable). A series of US Supreme Court cases in the past 10 years have cast a shadow over the patentability of software (See *Alice Corporation Pty. Ltd. v. CLS Bank International*)[5] and diagnostic methods (See *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*[6] and *Association for Molecular Pathology v. Myriad Genetics, Inc.*).[7] Successfully navigating these patentability hurdles is often a critical part of protecting the substantial investments that companies make in bringing their digital health solutions into the marketplace. Some recent US Supreme Court and Federal Circuit cases have begun to chip away at the patentability hurdles for diagnostics innovation (See *Hikma Pharmaceuticals USA Inc. v. Vanda Pharmaceuticals Inc.*[8] and *CardioNet, LLC v. InfoBionic, Inc.*)[9] and the current expectation is that future cases will continue to swing toward protection of this important area of innovation. And in other jurisdictions around the world, computational software driven innovations face similar hurdles toward patentability.

Copyrights can be used to protect software, including code for learning platforms like various machine and deep learning models. Copyrights can also be used to protect databases and some types of data content that which is itself original (e.g., structured compilations of genomic sequencing data, structured compilations of images, audiovisual recordings, detailed diagrams, etc.), but cannot protect factual data (e.g., raw genomic sequencing data, metabolite data, proteomics data, etc.). However, there may be other legal mechanisms that can be used to protect factual data, such as contract law and trade secret protection.

Trade secrets

Because of the current limitations of patent law, trade secret protection plays an outsized role in protecting digital health innovation relative to other industries. But trade secret law has inherent limitations that make it less protective of innovation than patents. For example, trade secret law does not protect against third parties independently developing identical solutions (i.e., digital health innovations) and it requires that the trade secret owner mark their trade secrets and demonstrate that they are taking active measures to ensure that their trade secrets are not misappropriated.

Data rights

Digital health solutions tend to both generate and utilise large quantities of health data, therefore, data rights are a vital component of digital health IPRs that needs to be protected. This is particularly true for digital health solutions that are powered by AI/ML algorithms as the accuracy of their predictions are largely determined by their training using large quantities of quality training data.

As discussed above, raw factual data is generally not protectable under copyright law, so the primary means used to guard data rights is currently with contract and trade secret laws. As the value of health data rights increases, the expectation is that the body of law dealing with data rights protection will also evolve to more adequately safeguard the rights of data owners.

Regulatory legal issues

Moving beyond IPRs, compliance with state and federal regulations is also essential for digital health companies seeking to successfully develop, market or implement digital health solutions in the US.

Data privacy

Continued access to medical data relies on patient trust and the laws and regulations that underpin that trust. As data gathering and access are critical components of most digital health solutions, it is vital that digital health companies adopt data privacy policies and infrastructure that are compliant with the data privacy laws and regulations of the jurisdiction(s) in which they operate.

In the United States, the most pertinent data privacy laws are the Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA). The jurisdictional boundaries of HIPAA and CCPA are carved out based on both the entity gathering the data (HIPAA Covered Entities and their Business Associates) and the legal residence of the individual whose data is being gathered. That is, HIPAA only applies to a statutorily defined group of Covered Entities such as health plans (e.g., health insurance companies, Medicare, Medicaid, etc.), healthcare clearinghouses (e.g., billing service, community health information

systems, etc.), and healthcare providers (e.g., physician, clinic, hospitals, pharmacies, etc.) that are considered traditional healthcare data custodians. Importantly, this leaves a coverage gap for non-traditional healthcare data custodians such as the technology companies (e.g., Amazon, Apple, Facebook, Google, etc.) that have recently entered the healthcare marketplace through their IoT and mobile app product offerings that can diagnose and treat healthcare-related issues. The first state to attempt to fill the HIPAA coverage gap was California when it enacted the CCPA in 2018. The CCPA provides privacy rights and consumer protection for data obtained from residents of California irrespective of the type of business.

Generally, both HIPAA and CCPA regulate how businesses collect, handle and protect an individual's personal information (PI) to ensure their privacy and give them control over the sharing (informed consent) of their PI with third parties.

FDA regulatory

Another set of regulations that digital health companies need to consider are those that regulate the safety and efficacy of digital health solutions. The Federal Food, Drug and Cosmetic Act (FFDCA) and related laws are federal statutes that regulate food, drugs, and medical devices. The FFDCA is enforced by the US Food and Drug Administration (FDA) which is a federal agency under the US Department of Health and Human Services (DHHS).

Depending on whether the digital health solution is a device, system or software, the FDA may enforce a number of different regulations and programs, including: 510(k) certification; Premarket Approval (PMA); Software as a Medical Device (SaMD); Digital Health Software Pre-certification Program (Pre-Cert Program); and Laboratory Developed Test (LDT) regulated under the Clinical Laboratory Improvement Amendments (CLIA) program. One technology area of focus for the FDA recently is AI/ML-powered digital health software, which is dynamic by design and thus poses particular challenges for the FDA as the current regulatory regime is based on software being static by design. The FDA recently launched a Digital Health Center of Excellence to further the advancement of digital health solutions and address the unique regulatory issues they pose.[10]

State-specific practice of medicine laws (telehealth and virtual health)

For telehealth and virtual health companies that provide physician consultations across state lines, the Interstate Medical Licensure Compact Commission (IMLCC) regulates the licensure of physicians to practice telemedicine in member states.

The Interstate Medical Licensure Compact (IMLC) speeds up the licensure process for physicians practising telemedicine as it eliminates the need for them to individually apply for licences in each state they intend to practice in by allowing them to obtain an IMLC licence that is valid in all states that have joined the compact. The following states have joined the IMLC: Alabama; Arizona; Colorado; Idaho; Illinois; Iowa; Kansas; Maine; Maryland; Michigan; Minnesota; Mississippi; Montana; Nebraska; Nevada; New Hampshire; Pennsylvania; South Dakota; Tennessee; Utah; Vermont; Washington; West Virginia; Wisconsin; Wyoming; and the District of Columbia and Guam.[11]

The Stark Law and Anti-Kickback Statutes

Telehealth and virtual health providers who enter into business arrangements with third parties that incentivise care coordination and patient engagement are also subject to federal Stark Law and Anti-Kickback Statutes (AKSs).

The Stark Law (or physician self-referral law) prohibits referrals by a physician to another provider if the physician or his immediate family has a financial relationship with the provider. The AKS, meanwhile, bars the exchange of remuneration (monetary or in kind) for referrals that are payable by a federal healthcare program like Medicare.

These laws provide another necessary consideration for telehealth companies as they can hinder opportunities for large health systems and companies to work together and to help smaller systems and hospitals develop their own platforms or take part in a larger telemedicine network.[12]

State and federal medical reimbursement laws and regulations

2020 has been a banner year for telehealth. Even before the COVID-19 pandemic, the remote care delivery model had been gaining traction among patients, particularly those who have grown up with technology.

Currently, all 50 states and the District of Columbia now provide some level of reimbursement coverage for telehealth services for their Medicaid members. At the federal level, the Mental Health Telemedicine Expansion Act was passed as part of the Omnibus Appropriations and Coronavirus Relief Package and the CONNECT for Health Act of 2019 and has been introduced but not passed.

Conclusions

The digital health sector experienced explosive growth even before the COVID-19 pandemic accelerated its adoption by mainstream payors, providers and patients. With the continued rapid pace of change in digital health, the expectation is that the delivery of healthcare will continue to transform. Within this transformation there will be some common themes.

The ability to gather data, generate clinical insights and transform those insights into actionable clinical solution(s) will form the foundation of value creation within digital health. In this paradigm, data access becomes the new "oil rush" as data will fuel the analytics engines behind many future digital health solutions. As a result, traditional technology players such as Amazon, Apple, Facebook and Google, may create substantial competition for traditional healthcare providers. It remains to be seen whether those advantages will translate to success in the digital health marketplace.

Clinical adoption of digital health solutions will continue to be a challenge as there are significant clinician concerns about how to safely integrate these solutions into their day-to-day practice. Moreover, digital health companies must navigate the myriad of state and federal regulations/laws relating to data privacy, FDA regulatory, practice of medicine, and medical reimbursement in order for their solutions to be even accessible by clinicians in the first place.

Lastly, there are brewing geopolitical factors that may impact how well digital health companies succeed in the marketplace. Regional regulations on health data access and usage (e.g., General Data Protection Regulation (GDPR), HIPAA, CCPA, etc.), reimbursement and product approval are additional requirements to contend with for companies that are foreign to the jurisdiction to contend with. Also, many countries have begun to aggressively invest in the gathering of healthcare data (especially whole genome data) on a national level, which can potentially be leveraged to

give domestic companies an edge over foreign ones. Examples of this are the UK Biobank Whole Genome Sequencing Project and Beijing Genome Institute (BGI) Million Chinese Genome Project. It is conceivable (and likely) that the UK and China will implement data access policies that specifically benefit domestic digital health companies to give them a home-grown advantage.

Endnotes

1. https://www.globenewswire.com/news-release/2020/11/17/2128470/0/en/Digital-Health-Market-Size-to-Hit-Around-US-833-44-bn-by-2027.html#:~:text=The%20global%20digital%20health%20market,27.9%25%20from%202020%20to%202027.
2. Stanford University School of Medicine (2017). "Harnessing the Power of Data in Health, Stanford Medicine 2017 Health Trends Report". Retrieved from: https://med.stanford.edu/content/dam/sm/sm-news/documents/StanfordMedicineHealthTrendsWhitePaper2017.pdf.
3. Amwell (2020). "From Virtual Care to Hybrid Care: COVID-19 and the Future of Telehealth". Retrieved from: https://static.americanwell.com/app/uploads/2020/09/Amwell-2020-Physician-and-Consumer-Survey.pdf.
4. Harrer, *et al.* "Artificial Intelligence for Clinical Trial Design." *Trends in Pharmaceutical Sciences* 40.8 (2019): 577–591.
5. https://www.supremecourt.gov/opinions/13pdf/13-298_7lh8.pdf.
6. https://supreme.justia.com/cases/federal/us/566/66/.
7. https://supreme.justia.com/cases/federal/us/569/576/#:~:text=Assoc.,Justia%20US%20Supreme%20Court%20Center.
8. https://www.scotusblog.com/case-files/cases/hikma-pharmaceuticals-usa-inc-v-vanda-pharmaceuticals-inc/.
9. https://law.justia.com/cases/federal/appellate-courts/cafc/19-1149/19-1149-2020-04-17.html.
10. https://www.fda.gov/news-events/press-announcements/fda-launches-digital-health-center-excellence.
11. https://intouchhealth.com/half-of-the-country-has-joined-the-telemedicine-licensure-compact/.
12. mHealth Intelligence (2020). "Stark Law Changes Should Benefit Telehealth, Remote Patient Monitoring". Retrieved from: https://mhealthintelligence.com/news/stark-law-changes-should-benefit-telehealth-remote-patient-monitoring.

Roger Kuan is a Partner at Norton Rose Fulbright and US head of the Precision Medicine and Digital Health Practice Group, where he counsels companies that are uniquely positioned in the convergence of the life/medical sciences and technology industries on how to successfully navigate the complexities of the intellectual property (IP), data rights and regulatory challenges they encounter.
Roger has extensive experience in IP strategy and portfolio management (utility/design patents, trademarks, copyrights, and trade dress), data rights strategy, licensing and technology transactions, freedom-to-operate clearances, enforcement, monetisation, IP due diligence, and dispute resolution. His practice is focused in the life sciences sector (e.g., research tools, analytical instrumentation/software, digital therapeutics, medical devices, diagnostics, biomanufacturing equipment, etc.) with an emphasis in emerging technologies such as precision medicine (e.g., genomic sequencing platforms, AI/ML, computational genomics/bioinformatics, molecular diagnostics, companion diagnostics, etc.), digital health (e.g., mobile apps, clinical decision support, software, AI/ML imaging diagnostics, wearables, etc.) and 3D printing/bioprinting.

Norton Rose Fulbright
555 California Street
Suite 3300
San Francisco, 94104
California
USA

Tel: +1 628 231 6800
Email: roger.kuan@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

David Wallace is a member of the Johnson & Johnson Law Department, and Group Leader of the Health Technology Team. In his role as Group Leader, David is primarily responsible for day-to-day activities regarding the patent aspects of the health technology initiatives across the Johnson & Johnson Family of Companies.

Johnson & Johnson
510 Cottonwood Drive
Milpitas, California 95035
USA

Tel: +1 408 273 5101
Email: dwalla34@its.jnj.com
URL: www.jnj.com

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3500+ lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

Recognised for our industry focus, we are strong across all the key industry sectors: financial institutions; energy, infrastructure and resources; transport; technology; life sciences and healthcare; and consumer markets. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

www.nortonrosefulbright.com

At Johnson & Johnson, we believe good health is the foundation of vibrant lives, thriving communities and forward progress. That is why for more than 130 years, we have aimed to keep people well at every age and every stage of life. Today, as the world's largest and most broadly based healthcare company, we are committed to using our reach and size for good. We strive to improve access and affordability, create healthier communities, and put a healthy mind, body and environment within reach of everyone, everywhere. We are blending our heart, science and ingenuity to profoundly change the trajectory of health for humanity.

www.jnj.com

The Rise of Digital Therapeutics and Corresponding Legal, Regulatory, and Policy Landscape


Jason Novak


René Quashie

Norton Rose Fulbright
Consumer Technology Association (CTA)

Digital therapeutics, of DTx, is a subset of digital health that, as defined by the Digital Therapeutics alliance [Digital Therapeutics Alliance; https://dtxalliance.org (2020)] focuses on "evidence-based therapeutic interventions driven by high-quality software programs to prevent, manage, or treat a medical disorder or disease". Over the past few years, DTx has quickly grown as a new platform for addressing the treatment, management, and/or prevention of various diseases. Technological advancements, to go along with the focus on multi-modal and data-driven solutions, has quickly elevated DTx into mainstream Healthcare discussion.

As with any emerging technology, particularly in healthcare, legal and regulatory policy issues often follow the emergence. However, DTx is an example of a "convergence industry" in that DTx is not the child of one industry, healthcare, but two, healthcare and tech.

As we have discussed in previous articles, digital health is a convergence of typically disparate industries: tech; and healthcare. Each industry encounters issues unique to their industry, particularly in the areas of intellectual property, data rights, and regulatory. Beyond unique issues, perspectives on these areas are different for each industry as well. Take open-source (OS) software as one of many examples. In tech, OS is often revered as the industry standard by which to operate, which has in turn strongly impacted the developers that create software solutions. In healthcare, not so much. But why?

In tech, the "how" something works is not as important as "what" it does. In healthcare, both the "how" and the "what" are fundamental to customer adoption, particularly with the regulatory underbelly that permeates healthcare innovation. That cultural difference can and has impacted perspectives in these disparate industries when applied to OS strategy.

As such, given that digital health is a combination of both tech and healthcare, it is often the case that almost all entities in the digital health world will have strategic (often legal) "blind spots" based on their experience leading up to the endeavour.

DTx is no different, especially as it applies to intellectual property, data, and regulatory considerations. As such, we will focus on those considerations in the world of DTx, and introduce some points to keep in mind as you consider your overall development strategy.

Legal Considerations

The legal considerations for DTx development are numerous and varied. Some of those considerations are standard fare for any innovation and will not be discussed. Others are industry-unique. Below, we will focus on a couple of unique considerations: intellectual property (IP); and data.

Intellectual property

IP strategy is industry specific. It is industry specific because markers exist within each industry that add up to a corresponding impact on IP strategy. Moreover, IP strategy is company specific. It is company specific because markers exist within each company that add up to a corresponding impact on IP strategy. Essentially, this means that IP strategy is *ad hoc*, not formulaic. As such, areas such as invention harvesting and invention protection must necessarily differ for each industry, and each company inside each industry. Anything less may result in a less sophisticated and insufficiently curated strategy than the specific DTx business or entity deserves.

Invention harvesting

Invention harvesting is the process by which IP experts interact with innovators to identify potential inventive ideas, and develop a strategy by which to protect them. In mature industries, such processes can be more formulaic because, for example, developers have been regularly educated on what to look for, and have had more experience capturing and defining those innovations. In growth industries, such processes are a bit less formulaic because, for example, developers have received little or no education on what to look for and, therefore, have less experience capturing and defining those innovations. In convergence growth industries (i.e., DTx), the issues become even more acute. Beyond the reality that the process is not formulaic at all, developers have received little or no education, and developers have nearly no innovation capture experience, the IP experts in these convergence spaces are few and far between. What can result is a situation of the blind leading the blind. Moreover, the developers often come from either side of the convergence. Therefore, beyond lacking the understanding of IP capture in the convergence space, many developers are biased by previous learnings and experiences on one or the other side (tech or traditional healthcare), making the task more difficult by having to educate while also breaking defined habits of traditional thinking. Again, think open source (OS) in a healthcare context. If you are a developer from traditional tech, what is your philosophy about OS? Now compound that by having leadership primarily having experience in traditional healthcare. Now compound that by placing these divergent philosophies and experiences in a DTx company, one for which neither has substantial experience. How would OS strategy be defined with those voices in the room?

So how does the tech *vs.* healthcare dichotomy affect invention harvesting? A better way to define the problem is to think

of a car. The hood of the car covers features of the car from public viewing. Those features above the hood are clear for all to see. Those features under the hood are not. Those features above the hood equate to features that may be, for example, customer facing, patentable at least to a degree depending on individual national IP laws, or have strategic value in the market if patented instead of maintained as confidential. Those features under the hood, by contrast, may be, for example, non-customer facing, non-patentable in key countries, or have strategic value in the market if maintained as confidential or a trade secret. Is that "hood line" always in the same place? Absolutely not. Can that "hood line" vary considerably? Absolutely. One of the big reasons is the industry of focus. So, let's look at this "hood line" in the context of traditional tech and healthcare.

As discussed above, traditional tech customers are generally concerned with "what" a product does, whereas traditional healthcare customers are generally concerned with both "what" a product does and "how" a produce works. Moreover, tech products are typically very transient, with innovation advancing rapidly, though often very iteratively, in most cases quicker than patent filings can be prosecuted to issued patents.

Healthcare, by contrast, often innovates and builds products for the long term, which is essentially necessary as the time to market for healthcare products are longer, and the accompanying and difficult regulatory approval requirements making iterative innovation less of a focus. As such, the timing for prosecuting patent applications more aligns with product life and feature stability.

Accordingly, in tech, less of a focus on "how" keeps many features under the hood. For example, with phone apps, customer expectations are geared around what an app does, not why it works. As such, typical public disclosure requirements are minimal. Add to that the transient nature of product development, and one can see why the "hood line" in tech is very high, with more under the hood than over it.

By contrast, the culture in healthcare substantially lowers that "hood line". In healthcare, there is a significant focus on the "how", not only from a customer expectation standpoint, but from a regulatory requirements standpoint as well. Thus, healthcare products are less transient. Add to that the publication-first culture of healthcare innovators in private companies, universities, research institutes, and hospital systems alike, public disclosure requirements and customer expectations are substantially higher. As a result, the "hood line" drops greatly relative to tech, resulting in more publicly facing features in healthcare products than tech products and a greater need to proactively secure rights to those features.

How does this affect the convergent DTx industry? First, as stated before, DTX companies often include both traditional tech and traditional healthcare leadership, bringing with them these traditional philosophies. Second, in our shrinking and increasingly connected world, these employees come from various territories around the world that have IP laws that can differ, sometimes widely, from each other. Third, the "ratio" of tech innovation to healthcare innovation is unique to each DTx company. The result is a "hood line" that often sits between these two traditional industries, in a gray zone for which neither is familiar. Therefore, counselling in the DTx space is essential to educate all these parties in an effort to define that line in the most appropriate and sophisticated way.

Finally, another increasingly influential variable is artificial intelligence/machine learning (AI/ML). AI/ML is a great example of technological advancement in one traditional industry (tech) heavily influencing healthcare. While AI/ML has conceptually existed for years, overall technological advancement of underlying software innovation and the digital marketplace has brought AI/ML to the forefront in healthcare as a feasible feature to generate unique insights never before possible. However, this only reinforces the dichotomy. While this discussion is complex enough to deserve its own article, it can be boiled down to a fundamental problem: tech's traditional view on IP protection for AI/ML likely will not align with the needs and opportunities in a DTx framework. For example, while traditional Tech may view the IP strategy as a patent *or* trade secret approach, DTx offers the opportunity at both patent *and* trade secret protection for these AI/ML-based solutions. Again, as stated above, sophisticated counselling in the DTx space is needed to understand AI/ML's impact on the corresponding "hood line".

Data considerations

As is apparent in recent months and years, DTx will continue manifesting throughout the healthcare industry. If the COVID-19 pandemic has taught us anything, it is that companies, healthcare providers, and health systems that have figured out how to maintain a digital infrastructure are more nimble and more capable of adapting to changes in healthcare delivery while driving adoption for the same. Given that reality, regardless of how complex our constantly evolving healthcare industry may seem to get, there is a common theme: data is king and the proper generation, acquisition, maintenance, transaction and/or use of data is essential to a successful DTx endeavour. As a result, to continue being relevant and adapting to the new operating reality, companies must focus on establishing a well-developed data strategy to execute a DTx endeavour. While there are many considerations, we will touch on only three in detail.

1. First Consideration: Know your industry and corresponding "blind spots"! As we have discussed previously, the convergence of typically disparate industries – tech and healthcare – to form DTx, converges issues unique to each industry. For example, tech can deal with data transactions, data privacy, and cybersecurity on a regular basis. Healthcare traditionally has not, at least not until digitisation brought about the concept of using and transacting with personal health information under HIPAA and other laws. Healthcare must contemplate FDA oversight and reimbursement considerations on a regular basis, while tech traditionally does not. Therefore, these industries have historically functioned in parallel: tech, focusing on moving fast to create the best, most innovative products; while healthcare, which is highly regulated and appropriately risk averse, concentrates on assessing every potential consideration before implementing a change.

   Recognising the disparate nature of this convergence will give DTx leaders the ability to recognise the strategic (often legal) "blind spots" based on their experience leading up to the endeavour. Knowing what you do not know is the first step to "cleaning up your house" as it relates to data strategy.
2. Second Consideration: Understand use/consent requirements! Healthcare data is exceptionally valuable to both the patient and the data-procuring company. Given its value and heavy regulated nature of that data, one must have permission to use healthcare data for a desired purpose. Regardless of whether the healthcare data is generated or acquired by the data user, the data user must have the consent of the data's ultimate owner, i.e., the patient, to use that healthcare data. In the cases where healthcare data is acquired from a third party, the data user must also have the consent of the third party to use the healthcare data for a desired purpose. Often, consent from a third party

(e.g., a healthcare data warehouse or aggregator) comes via a data transaction, where the data user can compensate, in some form, the third party to acquire the healthcare data for the desired purpose. Of course, the consent between data owner and data user will come via the data owner providing consent to this third party to transact the data to parties such as the data user. It is worth noting that a healthcare data warehouse or aggregator does not solely mean data mines such as personal genomics companies 23andMe and Ancestry. It also includes traditional entities such as hospitals and hospital systems, universities, research institutes and pharmaceutical companies. For simplicity, we will refer to these types of entities as Healthcare Data Aggregators (HDAs). Consent can come in a variety of ways, but it is critical to be able to demonstrate such consent for any downstream data use.

3. Third Consideration: Understand the true playing field when transacting with sophisticated entities! HDAs, through a data transaction, look to benefit from their held healthcare data. A benefit to a HDA can be in the form of, for example, direct remuneration, royalties from data user revenue, milestone payments (commercial and revenue milestones), equity in data user's company, and access to data user's analytical results. In cases where both parties are subject to some form of collaboration, joint venture or co-development agreement, profit can also include some ownership of co-developed intellectual property with the data user.

Moreover, given that most HDAs are likely to be large and traditionally sophisticated, negotiation leverage can be skewed in the HDA's favour. However, given the convergent nature of digital health, and DTx by extension, depending on the type of HDA, that sophistication may not carry to data rights transactions. The digitisation of healthcare has been rapid for everyone, and often the larger the entity, the less nimble it can be to the rapid industry changes. To a degree, that is why the start-up model works and has been successful over the years to introduce innovative technology to the healthcare industry, if not all industries.

Consider a personal genomics HDA that builds its business model around these transactions. Its sophistication and experience with these data transactions can be somewhat assumed. In fact, some may have fairly set data transaction terms determined over time and experience, therefore leaving little room for negotiation.

By contrast, some traditional entities (e.g., hospital systems, universities, research institutes, big pharma) may have general sophistication, but that may not stretch to data transactions. For example, being a sophisticated healthcare research institute does not inherently mean that said institute has any deep experience in healthcare data transactions. Additionally (and noteworthy), these sophisticated entities often operate amidst internal silos, where the portion of the organisation generating data may not be the same group that understands its value, understands what parameters exist around these data (e.g., consent limitations), and has business acumen to transact on these data. Since digital health is a convergence of typically disparate industries, as discussed above, "blind spots" can exist for even the most "sophisticated" entities.

Do note that while we discuss "blind spots", use/consent, and sophisticated entities as considerations, more considerations definitely exist. One example includes multiple data transactions, the requisite time and cost, and the impact one bad transaction can have on the entire platform. Another is the regulated nature of healthcare, discussed more below. The take-away here is that a data strategy needs to be formed early, before entering discussions and building products. The viral impact of a spotty data strategy can set back companies for years. As such, if the experience and resources do not exist in-house, you should seek help from outside resources.

Regulatory Considerations

The U.S. healthcare regulatory environment for DTx is evolving. From pathways to market to insurance coverage and reimbursement to privacy, federal regulators are wrestling with ways to regulate DTx.

Food and Drug Administration (FDA)

Digital therapeutics are generally regulated as software by the FDA under the agency's software-as-a-medical-device (SaMD) category and are subject to regulatory obligations much like conventional medical devices. In that sense, DTx is no different than other digital health solutions whose regulatory paradigm is largely based on the framework governing medical devices. As defined under FDA law, a medical device is an "instrument, apparatus, implement, machine, contrivance . . . or other similar or related article, including any component, part, or accessory" which, among other things, is intended for use in the diagnosis, treatment, cure, mitigation, or prevention of a disease or condition, or intended to affect the structure or function of the body.[1] Section 3060 of the Cures Act excludes from the definition of "device" software functions intended for activities such as healthcare facility administrative support, healthy lifestyle maintenance, or serving as electronic patient records, so long as the function is not intended to interpret or analyse them for the purpose of condition diagnosis, cure, mitigation or treatment.

When analysing software, there are a few questions for consideration:

- Is the solution intended for use in diagnosis, treatment, medical care, or disease prevention?
- If yes, is the solution exempt from the definition of a medical device under Section 3060 of the Cures Act? If so, then the solution is not considered a medical device.
- If not exempt under Section 3060, is the solution subject to "enforcement discretion"[2] under an applicable FDA guidance or policy? If yes, medical device obligations do not apply. If not, the solution may be regulated as a medical device.

If the software is considered a medical device, manufacturers must then determine a regulatory pathway to market. A 510(k) approval pathway, for example, applies to low/moderate risk devices (Class I or II), thus allowing for an abbreviated approval pathway, provided the applicant provide a predicate device to which the software is "substantially equivalent". A Premarket Approval (PMA) pathway, by comparison, has no predicate device, applies to the highest risk (Class III) of devices, and therefore requires clinical studies. *De Novo* Classification (*De Novo* 510(k)) provides the opportunity to classify novel medical devices that provide reasonable assurance of safety and effectiveness for the intended use, but for which there is no legally marketed predicate device. The *De Novo* 510(k) applies a risk-based classification process. Devices that are classified into Class I or Class II through the *De Novo* pathway may be marketed and used as predicates for future 510(k) submissions.

The pandemic saw the FDA relax some of its requirements allowing conditional approval of mental health-related DTx solutions during the public health emergency. As noted by the agency, this approach helps "expand the availability of digital health therapeutic devices for psychiatric disorders to facilitate

consumer and patient use while reducing user and healthcare provider contact and potential exposure to COVID-19 during this pandemic". For example, the FDA approved marketing of the first game-based digital therapeutic solution to improve function in children with attention deficit hyperactivity disorder.[3] The agency also approved a DTx designed to reduce sleep disturbance related to nightmares in adults who suffer from nightmare disorder or have nightmares from post-traumatic stress disorder.

According to data from the FDA, almost 65 DTx solutions have been approved by the agency with almost half of those approved after 2017. Most of the solutions were via the 510(k) pathway, with a much smaller subset coming through the *De Novo* or PMA pathways.[4] Some DTx have also received so-called Breakthrough Device designations, a programme designed to expedite the development and review of breakthrough technologies, while preserving the regulatory standards for the pathways discussed above.[5]

The FDA has recognised that its traditional regulatory paradigm was not designed for the kinds of software products on the market today. In response, the agency launched the Software Precertification (Pre-Cert) Pilot Program to help the agency develop a regulatory model for oversight of software-based medical devices that reflects current realities.[6] Under Pre-Cert, instead of evaluating individual SaMD products, the FDA is proposing to certify a company and its software development process for conformance to certain principles of excellence such as patient safety, product quality, and cybersecurity responsibility.

To the extent DTx solutions include AI/ML components, we note that the FDA recognises that AI/ML is fundamentally different from other SaMDs. The agency is in the process of developing a new regulatory paradigm specifically with AI/ML in mind. Under the traditional regulatory regime, products driven by AI/ML require repeated premarket review for software modifications – an unrealistic requirement given how frequently these modifications occur. Last year, the agency published an AI/ML action plan detailing the steps it will take in regulating the space, including supporting regulatory science efforts to develop methodology for the evaluation and improvement of ML algorithms, and advancing real-world performance pilots to provide additional clarity on what a real-world evidence generation programme would look like for AI/ML-based SaMDs.[7]

Insurance coverage of DTx

The Centers for Medicare and Medicaid Services (CMS), has not developed guidance regarding coverage and reimbursement of DTx, although the agency recognises a few reimbursement codes addressing collaborative care models that involve use of apps. Because CMS tends to be a market leader in terms of coverage and reimbursement, it is an important bellwether regarding if and how other insurance providers will cover emerging health technology like DTx.

The issue is that DTx does not fall under an existing Medicare benefit category. In other words, if a product or service cannot be placed in an established benefit category, Medicare will not cover and pay for that product or service. Some believe DTx can be shoehorned into one of the existing categories. For example, some have argued that DTx could fit into the durable medical equipment category, which among other things, requires an item to demonstrate it can withstand repeated use, has an expected life of at least three years, and is appropriate for use in the home.[8] The problem, however, is that DTx may not be able to meet the three-year expected life requirement, using just one counterpoint. Ultimately, these coverage debates underscore the issues with fitting 21st century technology into a coverage framework built for another time.

As reimbursement experts have noted "a CMS coverage pathway for DTx will require reimbursement rules for the time a clinician spends on remote monitoring of DTx data, akin to payment for a medical service, and the DTx product itself, akin to payment for a medical device or pharmaceutical".[9] There is hope on the horizon. Some have called for establishing a specific Medicare benefit category for DTx which would require an act of Congress. Difficult as that may seem, it has been done before as we can see in the examples of home infusion therapy and opioid use disorder treatment services. Medicare Advantage (the managed care portion of the Medicare programme) also allows plans far more flexibility to cover solutions such as DTx that do not yet have a benefit category through supplemental benefits.

On the private market side, the two largest pharmacy benefit managers in the U.S. established first-in-kind digital health formularies two years ago that provides a pathway for greater DTx adoption.

Security and privacy

Given that DTx solutions store and transmit patient data, privacy and security are key regulatory considerations for the category. Increasingly, cybersecurity issues are front and centre when it comes to connected or software-enabled devices. The FDA requires medical device manufacturers to comply with federal requirements to address risks, including cybersecurity. In acknowledging the increasing use of wireless and network-connected devices and the electronic exchange of medical device-related health information, the FDA published draft guidance in 2018 taking a tiered approach regarding cybersecurity risk.[10] Tier 1 devices (higher cybersecurity risks) are those capable of connecting (e.g., wired, wirelessly) to another medical or non-medical product, to a network, or to the Internet – and a cybersecurity incident affecting the device could directly result in patient harm for multiple patients. Tier 2 devices (standard cybersecurity risks) are medical devices for which the criteria for a Tier 1 device are not met.[11] The agency recommends that premarket submissions for Tier 1 devices include documentation showing how the device design and risk assessment incorporate certain design controls. For Tier 2 devices, the FDA recommends that manufacturers include documentation in their premarket submissions that either shows they have incorporated certain specific design features or provide a risk-based rationale for why design controls are not appropriate.

While the FDA has issued guidance regarding various aspects of cybersecurity including device design and the required documentation for premarket submissions, the agency does not require premarket security audits for medical devices.

Issues are just as complicated when it comes to privacy. The U.S. has a sectoral approach to privacy laws at the federal level unlike many jurisdictions around the world. This means that the privacy regulations that apply to data collected in the U.S. depend on the type and context of the data collected. The most well-known federal privacy law in the healthcare sector is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to "covered entities" and their "business associates". "Covered entities" consist of health insurance providers, healthcare clearinghouses (entities that assist the submission of claims to health insurance providers), and healthcare providers. "Business associates" are third parties that create, receive, maintain, or transmit protected health information (PHI) on behalf of covered entities. Many stakeholders, however (including DTx manufacturers), that collect and use PHI may not be covered under HIPAA's scope.

For those organisations, the Federal Trade Commission (FTC) is the primary federal regulator in data privacy and has broad jurisdiction over the data privacy and security practices of for-profit entities. The FTC gets its primary authority from Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce". The agency has used this broad jurisdiction to pursue enforcement actions against companies for engaging in "deceptive" practices by not complying with their own privacy policies, privacy settings, or other representations to consumers. The agency is particularly focused on organisations that use personal data not consistent with a consumer's reasonable expectations, including failing to implement reasonable security measures – which could be considered an "unfair" trade practice. The FTC also enforces the Health Breach Notification Rule that requires certain businesses not covered under HIPAA to notify their customers and others if there has been a breach of unsecured individually identifiable electronic health information. If all of the foregoing is not complicated enough, DTx stakeholders may also have to navigate a patchwork of state privacy laws that have been passed in the last few years.

Conclusion

Digital therapeutics is a wonderful example of innovation allowing for the convergence of disparate technologies that facilitate new frontiers of insights into our health. By synergising data streams from unique sources to produce novel insights, digital therapeutics solutions will provide the opportunity to look at health issues in a myriad of different ways as we seek new insights and potential solutions to existing diseases. But with that convergence comes greater opportunity for problems, legal and regulatory, from the start. As such, getting your legal and regulatory strategy right is essential to put you on the path to success.

Endnotes

1. 21 U.S.C. § 321(h).
2. An FDA policy in which even if a solution meets the definition of a medical device, the FDA chooses to not enforce its requirements because it has determined that the risk to patients of using the product is low.
3. https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-first-game-based-digital-therapeutic-improve-attention-function-children-adhd.
4. https://journals.plos.org/digitalhealth/articlefigure?id=10.1371/journal.pdig.0000008.t001.
5. https://www.fda.gov/medical-devices/how-study-and-market-your-device/breakthrough-devices-program.
6. https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-software-precertification-pre-cert-program.
7. https://www.fda.gov/media/145022/download.
8. https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/clm104c20.pdf.
9. https://www.healthaffairs.org/do/10.1377/forefront.20210510.303135/full/.
10 https://www.fda.gov/media/119933/download.
11. *Id.*

Jason Novak is a Partner in Norton Rose Fulbright's Precision Medicine and Digital Health Practice Group, where he focuses on advising entities, both large and small, on the various legal issues that can arise with emerging technologies in the healthcare and life sciences industries. Tech and biotech are traditionally disparate technologies that, when blended together to form many of our most exciting new technologies, bring forth a combination of unique and interrelated legal issues. Jason has extensive experience in IP strategy and patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in and out-licensing, freedom-to-operate, various types of due diligence, IP training, risk recognition and management, and dispute resolution. Prior to starting this practice, Jason was an IP Director for Thermo Fisher Scientific, where he managed worldwide IP needs in genetic sciences instrumentation and software.

Norton Rose Fulbright
555 California Street
Suite 3300
San Francisco, 94104
California
USA

Tel: +1 628 231 6800
Email: jason.novak@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

René Quashie is the first-ever Vice President of Policy & Regulatory Affairs, Digital Health at the Consumer Technology Association (CTA), the largest technology trade association in the U.S. with 2,000 member companies. Quashie provides guidance on key technical, legal and regulatory issues relating to digital health technology products, services, software and apps. Quashie also works on behalf of CTA's Health Division, which supports the health technology industry through advocacy, education, research, standards work, policy initiatives and more. Prior to CTA, Quashie was in private law practice at several national firms for two decades focusing his work on digital health and privacy. He earned his law degree from George Washington University.

Consumer Technology Association (CTA)
1919 S. Eads Street
Arlington
VA 22202
USA

Tel: +1 703 907 7600
Email: rquashie@cta.tech
URL: www.cta.tech

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3500+ lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

Recognised for our industry focus, we are strong across all the key industry sectors: financial institutions; energy, infrastructure and resources; transport; technology; life sciences and healthcare; and consumer markets. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

www.nortonrosefulbright.com

As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators – from start-ups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES® – the largest, most influential tech event on the planet. Member companies enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships.

www.cta.tech

Global Landscape of Digital Health: Impact on Healthcare Delivery and Corresponding Regulatory and Legal Considerations


Lincoln Tsang


Kellie Combs


Katherine Wang


Daisy Bray

Ropes & Gray LLP

Global Context

The World Health Organization (WHO) considers digital health – a broad umbrella term encompassing e-health, as well as developing areas such as the use of advanced computer sciences in the fields of "big data", genomics and artificial intelligence (AI) – to play an important role in strengthening health systems and public health, increasing equity in access to health services, and in working towards universal health coverage.

The emerging digital health industry therefore encompasses digital products or platforms that can monitor, analyse, educate or improve health. The industry can be segmented into telehealth, mobile health (mHealth), Artificial Intelligence (AI), digitalised health systems and electronic health records (eHRs), big data initiatives, analytics and more. The integration of digital health into national health systems and daily lives has become more ingrained. The COVID-19 pandemic has accelerated this integration, with increased funding and deployment of new technologies and care models to address challenges posed by the pandemic. Healthcare professionals provided remote video consultations, prescriptions were ordered via apps, and patients relied on digital screening questionnaires and other tools to inform their healthcare decisions. The pandemic, and the demonstration of the benefits of remote healthcare, gave fresh impetus for digital developments that, for a long time, had been discounted by many.

Unsurprisingly, the digital health market has grown significantly in recent years. The size of the digital health market exceeded US $141.8 billion in 2020 and is estimated to grow at approximately 18% between 2021 and 2027. Digital health technology will unquestionably have a significantly transformational impact on healthcare delivery and patient outcomes concerning such matters as early disease prevention and diagnosis, management and monitoring of chronic conditions, tailoring of medicines and treatment, lowering of healthcare costs and increased accessibility to healthcare.

Along with mHealth, eHealth has been defined by the World Health Organization as "the cost-effective and secure use of information and communications technologies in support of health and health-related fields, including health care services, health surveillance, health literature, and health education, knowledge and research". eHealth has enabled more efficient and responsive healthcare systems around the world and continues to improve and allow for cost and time savings.

Greater emphasis is increasingly placed on adjusting lifestyle to maintain wellness and prevent disease. Wearable trackers have historically focused on measures of fitness and wellness. Originating with counting steps, certain wearables can now monitor metrics such as sleep, reproductive health, calories burned, heart rate and even take electrocardiograms.

AI software with the capacity to perform operations analogous to learning and decision-making in humans has been increasingly applied in the pharmaceutical, medical technology and healthcare sectors to assist various stages of research and development, as well as treatment of patients. In order to meet the societal and patient needs of the 21st century, current research, development, and patient treatment will need to dramatically improve in efficiency. AI has the ability to streamline the process of translating a molecule from the initial inception to a market-ready product, to identify eligible patients for clinical trials, and to provide assistance, such as clinical decision support for providers, in the care setting. Big data-enabling companies to process and analyse large amounts of data generated post-market can mean better insight into how a new product works in the real world and so improve knowledge and accuracy of treatment choices.

The technological evolution based on convergence of biological, physical and mathematical sciences brings about significant legal and regulatory policy challenges. In general, national regulatory frameworks do not adequately address the distinct features and rapid pace of innovation of digital health technologies. To harness the full potential of these technologies, it is imperative that regulatory frameworks across the world evolve and harmonise to encourage innovation and allow for regulatory flexibility, while ensuring the core principles of quality, performance characteristics, safety and effectiveness. We discuss below some of those issues surrounding such technological advances.

Regulation and Enforcement

The emerging and constantly developing innovation of digital health poses regulatory challenges that are being met in varying ways across jurisdictions. In most jurisdictions, digital health is not regulated by a single bespoke legislation but by a number of different legal regimes. However, the national or regional regulatory and enforcement rules share the common theme that they are designed to achieve a high level of protection of human health and consumer interests.

Not all software used in the healthcare setting is considered to be a medical device. Countries or regions with a well-established regulatory regime for healthcare products have considered certain software to be regulated as a software medical device. The borderline classification takes account of the intended purpose or use of the software. The intended purpose is largely determined by the manufacturer and can be inferred from the label, the instruction for use and the promotional material related to a given software, among other sources depending on the jurisdiction.

The International Medical Device Regulators Forum ("IMDRF"), a consortium of medical device regulators from around the world, has defined software as a medical device ("SaMD") as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device". In the United States, the Food and Drug Administration ("FDA") has adopted this definition of SaMD in its regulatory framework for digital health, which has been evolving over the last decade. The FDA has been working to establish a new regulatory framework for digital health technologies that adopts a risk-based approach based on the intended use and functionalities of the product. The FDA's risk-based approach generally classifies digital health technologies into one of three categories: (1) a non-device, not subject to regulation (lowest risk); (2) a device for which the FDA will not enforce certain regulatory requirements, such as premarket authorisation (medium risk); or (3) a device subject to full regulatory oversight (highest risk), including premarket authorisation requirements as applicable.

In China, the National Medical Products Administration ("NMPA") formed its regulatory framework for SaMD in 2015. SaMD is typically classified as a Class 2 or a Class 3 medical device in China and is subject to the premarket authorisation requirements. In 2020, the NMPA published the draft amendment of the SaMD technical review guidelines. The draft guidelines emphasised the marketing authorisation holder's responsibility to establish oversight during the SaMD's total product life cycle. The higher risks the SaMD carries, the more stringent controls the marketing authorisation holder must adopt in the quality management system.

The EU regulatory framework similarly classifies medical devices according to their performance characteristics and intended use. Software must have a medical purpose for it to be so classified. European jurisprudence considers that a medical purpose covers an object intended by its manufacturer to be capable of appreciably restoring, correcting or modifying physiological functions in human beings. Such an assessment takes account of the composition of the product, the manner in which it is used, the extent of its distribution, its familiarity to consumers and the risks its use may entail. Classification of software is fraught with practical challenges because, unlike classification of general medical devices, it is not immediately apparent how these parameters apply to software, given that software does not ordinarily act on the human body to restore, correct or modify bodily functions. The Court of Justice of the EU ("CJEU") had ruled in Case C-329/16 SNITEM and Philips that software, of which at least one of the functions makes it possible to use patient-specific data for the purposes, *inter alia*, of detecting contraindications, drug interactions and excessive doses, is, in respect of that function, a medical device, even if that software does not act directly in or on the human body.

The new Regulation (EU) 2017/745 ("MDR") replacing Directive 93/42/EEC on medical devices reflects and expands the European jurisprudence on a medical purpose and defines a medical device very broadly to include, among others, any instrument, apparatus, appliance, or software intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specified medical purposes such as diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease.

Similarly, Regulation (EU) 2017/746 ("IVDR") on *in vitro* diagnostic medical devices ("IVDs") and repealing Directive 98/79/EC also defines an *in vitro* diagnostic medical device very broadly to mean any medical device which is, among others, a calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used *in vitro* for the examination of specimens, solely or principally for the purpose of providing information concerning such matters as a physiological or pathological process or state, the predisposition to a medical condition, prediction of treatment response or reactions.

Since MDR and IVDR were not directly applicable EU law instruments in the UK before its departure from the European Union, these regulations were not implemented in the UK domestic law. However, in September 2021, the UK Medicines and Healthcare products Regulatory Agency ("MHRA") launched a comprehensive public consultation on the future of medical device regulation in Great Britain. Similar to the MDR and IVDR, the overarching themes seek to create a robust, transparent and sustainable regulatory framework that addresses: (a) improved patient and public safety; (b) greater transparency of regulatory decision-making and medical device information; (c) close alignment with international best practice; and (d) more flexible, responsive and proportionate regulation of medical devices. The future framework for the UK for medical devices and IVDs is forward-looking to regulate such software technology by balancing between enhancing safety measures while incentivising innovation through earlier market access of an innovative medical device.

Adaptive AI technologies pose a challenge to existing regulatory frameworks because they are constantly evolving and learning. Read-out can be flawed due to quality of the source data used to develop the algorithm, resulting in algorithmic bias and a lack of contextual specificity, and thereby compromising patient safety. AI programmes use complex algorithms and black box deep learning for any person, including the initial programmer, to navigate. The recently proposed regulation for AI in the EU broadly defines it to include: machine-learning approaches; logic and knowledge-based approaches, including inference and deductive engines, reasoning and expert systems; statistical approaches; and search and optimisation methods. The proposed regulation classifies AI systems into three risk categories, namely:

- unacceptable-risk AI systems that present a clear threat to the safety, livelihoods and rights of people (e.g., subliminal, manipulative or exploitive techniques that could cause harm) will be banned;
- high-risk AI systems in various defined settings (e.g., systems utilising biometric identification in non-public spaces; systems that would put the fundamental individual rights and health of citizens at risk due to system failure) will be subject to strict requirements; and
- limited (where users can make an informed decision to continue or step back) and minimal risk (which represent only minimal or no risk for citizens's rights or safety) AI systems (e.g., AI chatbots) will be subject to minimal regulation.

The proposal has an extraterritorial reach and applies to providers placing on the market or putting into service AI systems in the EU, irrespective of whether those providers are established within the EU; users of AI systems located in the EU; and providers and users of AI systems that are located outside the EU (i.e. a third country) where the output produced by the system is used in the EU. Companies that use banned AI practices in breach of EU rules, or provide incorrect or misleading information to authorities, could face significant fines.

In China, the NMPA defines artificial intelligence/machine learning ("AI/ML") SaMD as software that leverages AI to process, measure, model and analyse medical device data for medical purposes. If the software processes non-medical device data (e.g., patient claims or lab reports), or processes, measures, models or analyses medical device data for non-medical purposes, or its core functionality does not include processing,

measuring, modelling or analysing medical device data, such software will not be regulated as AI/ML SaMD. The classification of AI/ML SaMD will depend on the maturity of the AI/ML algorithm being applied in medical practice and the intended use. If the AI/ML has not been widely applied in medical practice or if the intended use is to assist with medical decisions, the AI/ML SaMD will very likely be regulated as a Class 3 medical device.

In the United States, the FDA has also focused on the regulation of AI/ML technologies in recent years and released an Action Plan in January 2021 that outlines key actions for advancing the effort toward practical oversight of AI/ML software. These actions include: issuing guidance on the FDA's expectations for submissions related to software modifications; encouraging harmonisation of Good Machine Learning Practices; promoting user transparency and a patient-centred approach to regulation; supporting efforts for evaluating and improving algorithms to address issues such as bias; and working with stakeholders piloting real-world performance initiatives to better understand how AI/ML products are being used and to respond proactively to safety and usability concerns.

The FDA has taken some regulatory actions related to digital health technologies in recent years, though enforcement in this area remains low. For example, the FDA recently issued a warning letter to a company for marketing a smart monitor without seeking pre-market regulatory clearance. Additionally, to promote the uptake of digital health products during the COVID-19 pandemic, the FDA announced temporary policies to suspend enforcement of certain legal requirements for certain lower-risk digital health technologies, such as those treating psychiatric disorders. The FDA enforcement will likely increase in the future with the increased adoption of digital health technologies.

In the EU, Member States are responsible for enforcing the requirements set out in EU legislation governing medical devices and IVDs. The penalties to be applied must be effective, proportionate, and dissuasive. In the UK, the MHRA enforces regulatory compliance under the domestic law governing protection of consumer interests and public health. The MHRA's policy is to achieve compliance without resorting to enforcement activity wherever possible; it is only in the most serious or persistent cases that they take enforcement action.

Impact on Healthcare Delivery

The WHO has considered that digital health could revolutionise healthcare delivery, and should therefore be an integral part of each country's health priorities. Such health-related tools should be developed according to the principles of transparency, accessibility, scalability, replicability, interoperability, privacy, security and confidentiality.

The European Commission has identified robotics and AI as cornerstone technologies to improve health and care within the internal single market. The recent report on the State of Health in the EU concluded that only by fundamentally rethinking the EU health and care systems can one ensure that they remain fit-for-purpose. Accordingly, innovative solutions should be considered in response to changes in the demographics and multiple morbidities and the rising burden of preventable non-communicable diseases caused by risk factors such as tobacco, alcohol, and obesity, and other diseases including neuro-degenerative and rare diseases. Digital health would meet the objective of promoting research, disease prevention and personalised patient-centred health and care. Such digital solutions can increase the well-being and radically change the way health and care services are delivered to patients, if designed purposefully and implemented in a cost-effective way. One specific area is to standardise the specification for eHRs to facilitate cross-border care. As such, the European Commission has considered the need to review Directive 2011/24/EU on the application of patients' rights in cross-border healthcare and the relevant implementing decisions to advance the interoperability of eHealth solutions and to clarify the role of the e-Health Network in the governance of the e-Health digital service infrastructure and its operational requirements.

Outside the scope of this chapter, the reimbursement pathway for digital health technologies is currently unclear. That said, in recognition that digital health technologies are developed at an increasing pace, in the UK, the National Institute for Health and Care Excellence, NHS England, Public Health England, MedCity and Digital Health London have developed an evidence standards framework for digital health technologies to assist innovators and commissioners in understanding what good levels of evidence for digital health technologies would look like to ensure new technologies are clinically effective and offer economic value. In the United States, reimbursement for healthcare services provided remotely through telehealth and other digital health technologies have historically been limited; however, government and commercial payors are increasingly reimbursing such services, in part due to the realities of the COVID-19 pandemic.

Data Generation for Real-World Evidence

Observational studies are a fundamental part of epidemiological research to complement knowledge from randomised controlled trials and fill certain gaps, particularly where clinical trials cannot be conducted to characterise the clinical safety and efficacy profile as well as the therapeutic position of an innovative product in a real-world setting. Such a methodological approach has become more important in providing evidence on safety and effectiveness of vaccines and treatments for COVID-19 as it is critical to understand how exposure to certain medicines can affect the risk or the severity of infection with the circulating virus in the community.

eHRs and databases (including registries) containing other health-related data (claims, pharmacy) can support high quality observational research and pragmatic clinical trials, both of which can be important sources of real-world evidence. Integrating data from different sources creates a richer, more robust dataset than any one single source can yield. However, combining data from different sources can be a labour-intensive process due to challenges with data standardisation and interoperability.

In order to gain acceptance of such data sources by regulatory authorities as supportive evidence, data quality management should be prospectively defined and implemented with a focus on a core set of data elements and data systems to ensure integrity, completeness and security of the data sources.

Use of real-world evidence in product development has traditionally been limited by a lack of clear guidance from regulators or comfort with the reliability of the real-world data set. During the COVID-19 pandemic, regulators and industry have heavily relied on real-world data by necessity to understand the epidemiology and to assess potential treatment options. For example, in the United States, the FDA collaborated with a health IT vendor to launch a real-world evidence research project focused on the use of diagnostics and medications during the COVID-19 pandemic. The FDA has continued to gain comfort with real-world evidence, and has begun crafting a framework regarding how sponsors can utilise real-world evidence. Specific guidance from global regulators and increased comfort on the part of sponsors, regulators and other stakeholders will likely promote greater use of real-world evidence in the future.

Product Liability

In the EU, product liability rules under the Product Liability Directive 85/374/EEC aim at maintaining a fair balance between the interests of consumers and producers. Recent reviews of the Product Liability Directive have raised certain legally challenging issues arising from the fact that the distinction between products and services have been blurred in the context of digitalisation and AI. Some have commented whether the Product Liability Directive and civil liability regimes in the Member States are capable of addressing issues that may arise from such digitalised platform technologies.

In June 2021, the European Commission published an inception impact assessment roadmap on adapting civil liability rules to the digital age, AI and the circular economy. This initiative was prompted by the earlier assessment of the Product Liability Directive and addresses challenges that arise when liability rules are applied to such new technologies. The assessment emphasises that the liability framework should seek: (a) to provide legal certainty to companies about the risk they take in the course of their business; (b) to encourage the prevention of damage; and (c) to ensure injured parties are compensated. Accordingly, the liability rules should strike a fine balance between these competing objectives and promoting innovation.

The Commission also identified a number of ways in which software and AI might impact product liability and, hence, the shortcomings of the Directive in coping with the digital technologies. They include: (a) intangibility of digital products where digital content, software and data play a crucial role in ensuring the safety and functional characteristics of such technologies; (b) connectivity and cybersecurity, recognising that new technologies bring with them new risks such as openness to data inputs that may affect safety, cybersecurity risks, risks of damage to digital assets or privacy infringements; and (c) complexity of digital technologies, for example, within Internet of Things ("IoT") systems, makes it challenging for injured parties to identify the responsible producer.

The European Commission points out that importers are treated as producers for the purposes of the Product Liability Directive but that the digital age has brought changes to value chains. The Internet has enabled consumers to access services and buy products from outside the EU without there being an importer, and hence the risk that no one could be held liable under the Directive. Moreover, the specific characteristics of AI make it especially difficult to get compensation for damages under the Product Liability Directive and national civil liability laws.

The most recent ruling of the CJEU in Case C-65/20 *VI v KRONE-Verlag Gesellschaft mbH & Co KG* could be instructive in that it clarifies whether a physical copy of a daily newspaper (an information-sharing medium) can be regarded as a product for the purpose of the Directive in circumstances where the alleged defect was in relation to a health recommendation, which when followed could cause physical harm. CJEU has considered that the liability of service providers and the liability of manufacturers of finished products constitute two distinct liability regimes as the activity of service providers cannot be equated with those of producers, importers and suppliers that are covered by the Product Liability Directive. The ruling considers that a copy of a printed newspaper containing inaccurate health advice relating to the use of a plant, which, when followed, has proven to cause personal injury to the reader of the newspaper does not constitute a defective product within the meaning of the Product Liability Directive.

In the United States, a unified, consistent approach to product liability for digital health technologies has not emerged, in large part because these technologies are novel and product liability law is still evolving to catch up. Product liability is generally codified in state law, meaning that each state has different liability standards. Courts differ on the key question of whether software is even considered a product at all, or rather a service, which would then nullify any product liability claims. The learned intermediary doctrine, which is settled law in a majority of states, limits a device manufacturer's duty to warn of risks to treating physicians, who serve as "learned intermediaries" and assume the duty to convey those warnings to patients. As many digital health technologies empower consumers to make their own healthcare decisions without a physician, it remains to be seen what impact this has on product liability going forward. Digital health products also typically have multiple components, which complicates the determination of which party to target in a product liability suit. U.S. federal law does expressly preempt all state law claims, including product liability claims, directed at Class 3 medical devices (highest risk) that have successfully completed the premarket approval process unless those claims parallel federal requirements. As such, manufacturers of Class 3 medical devices have protection against state laws more rigorous than federal ones, though in practice manufacturers seeking to assert preemption often face challenges.

Conclusion

The digital health industry is dynamic, fast-growing and holds great promise for revolutionising healthcare across the world. There is significant regulatory uncertainty and global inconsistency around how digital health technologies should be regulated, as well as unclear reimbursement rules and policies.

Given that such technologies are increasingly embedded into healthcare delivery, the potential attendant risks that may arise from the design and implementation of such technologies could potentially be far-reaching in terms of exposure to liability claims. However, such a risk assessment will likely be complex as it should take account of the infrastructure of the healthcare system in which the technology is being applied, which may vary considerably country to country.

Acknowledgment

The authors would like to thank Jessica Band for her invaluable assistance in the writing of this chapter. Jessica is an associate in Ropes & Gray's FDA regulatory practice group and routinely advises life sciences companies on a wide range of FDA regulatory matters including product research and development, promotional compliance, post-market risk mitigation, and digital health. Jessica also routinely provides regulatory counsel for complex transactions, including mergers, acquisitions, and strategic collaborations, as well as public offerings of FDA-regulated companies, including drug, device, dietary supplement, and cosmetic manufacturers, and clinical research organisations. Prior to joining the firm, Jessica worked for Kaiser Permanente and the Advisory Board Company where she counselled hospitals and health systems on technology adoption and quality monitoring.

Dr. Lincoln Tsang is partner and head of Ropes & Gray's European Life Sciences Practice. A former senior regulator, he is qualified as a lawyer and a pharmacist with post-graduate training in toxicology and cancer pharmacology, and concentrates his practice on UK, EU and cross-border regulatory compliance and enforcement, including litigation, internal investigations and public policy matters affecting the life sciences industry. Lincoln advises clients on research and development strategies, product life cycle management, product acquisition, and risk and crisis management.

Ropes & Gray LLP
60 Ludgate Hill
London EC4M 7AW
United Kingdom

Tel: +44 20 3201 1500
Email: Lincoln.Tsang@ropesgray.com
URL: www.ropesgray.com

Kellie Combs, partner in Ropes & Gray's FDA regulatory practice group and co-chair of the firm's cross-practice Digital Health Initiative, provides legal and strategic advice to pharmaceutical, biotechnology, medical device, food and cosmetic manufacturers, as well as hospitals and academic institutions, on a broad range of issues under the Food, Drug, and Cosmetic Act and the Public Health Service Act. Kellie is currently advising several clients on issues related to the COVID-19 pandemic, including the deployment of digital health and telemedicine tools and the marketing of products authorised pursuant to FDA's Emergency Use Authorisation process.

Ropes & Gray LLP
2099 Pennsylvania Avenue, NW
Washington, D.C. 20006-6807
USA

Tel: +1 202 508 4600
Email: Kellie.Combs@ropesgray.com
URL: www.ropesgray.com

Katherine Wang is a partner in Ropes & Gray's life sciences group. Widely regarded as a leading life sciences regulatory lawyer in China, Katherine assists pharmaceutical, biotechnology, and medical device companies on a wide range of matters, including early-stage discovery, product registration, regulatory/GxP compliance, pricing, reimbursement, clinical studies, promotional practices, and product safety issues. Katherine provides day-to-day counselling on issues that life sciences companies face in relation to their interaction with agencies including the National Medical Products Administration ("NMPA", formerly the "CFDA"), the National Health Commission ("NHC"), the State Administration of Market Regulation ("SAMR"), and the Human Genetic Resources Administration of China ("HGRAC"), among others.

Ropes & Gray LLP
36F, Park Place
1601 Nanjing Road West
Shanghai 200040
China

Tel: +86 21 6157 5200
Email: Katherine.Wang@ropesgray.com
URL: www.ropesgray.com

Daisy Bray is an associate in Ropes & Gray's European Life Sciences practice and focuses on the regulation of pharmaceutical products and medical devices. Daisy advises on the boundaries of the ABPI and EFPIA Codes of Practice and UK and EU legislation in relation to numerous issues throughout a product life cycle including clinical research, advertising and promotion, authorisation, safety vigilance, pricing and reimbursement, use of social media and marketing materials. She also provides regulatory compliance advice, assisting with product-related investigations, public inquiries and resolving disputes arising from the decisions of regulatory bodies such as the Medicines and Healthcare products Regulatory Agency ("MHRA") and the European Medicines Agency ("EMA").

Ropes & Gray LLP
60 Ludgate Hill
London EC4M 7AW
United Kingdom

Tel: +44 20 3201 1500
Email: Daisy.Bray@ropesgray.com
URL: www.ropesgray.com

Balancing the Power of Data in Digital Health Innovation and Data Protection and Security in Pandemic Times


Dr. Nathalie Moreno


Johanna Saunders


Annabelle Gold-Caution


Lydia Loxham

Addleshaw Goddard LLP

1 Introduction

In the midst of the lingering COVID-19 pandemic, the United Kingdom (UK) and Europe's governments and private businesses alike have embarked upon unprecedented data-driven digital innovation and transformation initiatives regulated by and at times challenged by ever evolving data protection and security rules.

During the last two years of the pandemic, unprecedented swift developments in health technology both in the public and the private sector have enabled the UK to rise to the urgency of unexpected healthcare demands. Contact tracing apps that could be quickly made accessible to the public to shore up defences against COVID-19 and protect healthcare infrastructure; accelerated research and development between multiple organisations and jurisdictions and expedited clinical trials in the development and roll out of vaccinations; the growth of online healthcare providers where premises were closed or inaccessible to patients; and the increase in sales of smart healthcare devices allowing patients greater involvement and control over their own health and health data have all been benefits arising out of this crisis.

However, to gain user support for these advances, developers must keep an eye on their data protection obligations under the UK General Data Protection Regulation (**UK GDPR**), ensuring that they provide adequate processing information to users, have a lawful basis for their processing, make full use of data protection impact assessments so they can consider the risks inherent in their products and embed data protection and security at the design stage and by default. As highlighted by the Information Commissioner's Office (**ICO**), the effectiveness of data-driven technology relies in part on public trust and transparency is very important to developing and maintaining that public trust.[1]

2 Data Sharing in Healthcare

2.1 Contact Tracing

2.1.1 The NHS COVID-19 App

As the COVID-19 outbreak has prompted a wide range of responses from governments around the world, contact tracing apps have emerged as a double-edged digital weapon, both as a containment measure and as a privacy challenge. In the UK, the NHS COVID-19 app, the official contact tracing app for England and Wales and a vital part of the NHS Test and Trace service in England, and the NHS Wales Test, Trace, Protect service, have been fraught with privacy concerns since their launch. Clearly, the access and use of health and location data of millions of individuals by the NHS, during a sustained period of time since the start of the COVID-19 outbreak, has raised legitimate concerns of equally unprecedented mass surveillance of society at large.

Contact tracing has become a key tool in the battle against COVID-19 to alert people that they had come into contact with someone who had tested positive for the virus, check symptoms, book or order tests, and count isolation days, in an attempt to slow the spread of the virus. The hasty development of the NHS COVID-19 app and the initial absence of the data protection impact assessment (**DPIA**) released late in August 2020 by the UK Department of Health and Social Care (**DHSC**) and criticised for lacking transparency, both undermined public trust and negatively influenced perceptions of app efficacy. Since then, lessons were learned and the DHSC has regularly been updating the DPIA which is publicly available online as new functionalities were added to the app. In particular, the use of the app's QR scanner to check into places like restaurants, pubs, venues in the tourism and hospitality sector but also into close-contact businesses such as barbers, tailors or beauticians, raised serious privacy concerns that information about staff, customers and visitors, which constitutes personal data under the UK GDPR, may not be stored or used for contact tracing purposes only creating another occurrence of mission creep. Whilst use of the app was a formal legal requirement for some venues prior to 19 July 2021, businesses may still be able continue data collection by relying on legitimate interests as the legal basis for the processing.

2.1.2 ICO Guidance

On 4 May 2020, the ICO released its guidance on COVID-19 contact tracing: data protection expectations on app development, which confirmed the paramount importance for developers of contact tracing apps to perform a DPIA prior to implementation, given that the processing is likely to result in a high risk to the rights and freedoms of individuals.[2] Further, DPIAs should be continuously reviewed and updated while the contact tracing technology is in use.

In addition, on 2 July 2020, the UK ICO published its guidance on "Maintaining records of staff, customers and visitors for contact tracing purposes" (please see: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/maintaining-records-of-staff-customers-and-visitors-for-contact-tracing-purposes/) and made clear that the information collected could not be used for direct marketing or other business purposes. Yet in October 2020, the ICO launched an investigation into a number of digital contact tracing service providers to assess their data protection practices, including direct marketing, as concerns emerged that unlawful sharing and sale of information collected by QR codes was taking place with marketers, credit companies and insurance brokers.

2.1.3 ICO Enforcement

On 18 May 2021, the ICO announced that it had issued a monetary penalty notice to, and imposed a fine of £8,000 on, Tested.me Ltd, a contact tracing QR code provider, following various complaints from individuals for its sending of nearly 84,000 direct marketing emails without adequate valid consent, in violation of Regulation 22 of the Privacy and Electronic Communications Regulations 2003 (**PECR**).[3]

The ICO took the opportunity to remind providers of its guidelines including:

- Incorporating a data protection by design approach for the development of new products from the start.
- Ensuring that privacy policies remain clear and simple so as to be easily understood.
- Not retaining data collected for more than 21 days.
- Not using the data collected for marketing or any other business purpose.
- Complying with the latest ICO's online guidance.

2.2 The UK NHS Digital GPDPR Programme

2.2.1 Genesis of the GPDPR

NHS Digital is the national custodian for health and care data in England and has responsibility for standardising, collecting, analysing, publishing and sharing data and information from across the health and social care system, including general practice. In April 2021, the Secretary of State for Health and Social Care issued a Direction under the Health and Social Care Act 2012 requiring NHS Digital to establish and operate an information system for the collection and analysis of general practice data for health and social care purposes.

To date, NHS Digital collects patient data from general practices using a service called the General Practice Extraction Service (**GPES**). On 12 May, NHS Digital issued a Data Provision Notice to GPs to let them know that the GPES will be replaced by a brand new scheme, the General Practice Data for Planning and Research (GPDPR programme (https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/general-practice-data-for-planning-and-research) from 1 July 2021 with the aim of collecting pseudonymised GP data daily to support vital health and care planning and research).

During the pandemic, NHS Digital had been legally permitted to collect and analyse healthcare information about patients to enable the identification of those most vulnerable to COVID-19, the roll out of vaccines and for critical COVID-19 research. In practice, the data to be collected may not include patients' names and addresses but could include a patient's NHS number, date of birth and full postcode as well as information about mental health, domestic violence, treatments and addictions.

However, the principal difference between the GPES and the GPDPR programmes will not be the technology but rather the fact that, post-pandemic, the primary care data extracted through the GPDPR by NHS Digital is to be made available generally to third parties outside the NHS for research and planning. It is meant to involve a broader general purpose collection that would, through enhanced technology, enable faster access. The intention was that NHS Digital would pseudonymise the data before sharing, and such data could only be converted back to identifiable data in certain circumstances and where there is legal reason. Importantly, patients were entitled to opt out of the collection process completely or in part only of NHS Digital sharing their personal data, but were given a very short window of time to decide and very limited public information. In response to growing general concerns that not enough time had been given to let people know specific information about the service, its purposes, patient rights to opt out and that patient trust could be destroyed, the implementation date for the programme was moved from 1 July to 1 September 2021 to ensure that more time is allocated to speak with patients, doctors and health charities about the plans. However, it has now been postponed until 31 March 2022.

This latest initiative bore resemblance to the previous ill-fated "care.data" initiative, which also sought to share pseudonymised patient data collected by GPES with third parties, including commercial organisations outside the NHS, for research. This was shut down in 2016 following criticism of its failure to adequately inform patients of the programme and their right to opt out of collection. Unfortunately, lessons do not appear to have been learned in the intervening years, as concerns were again raised that patients had again been inadequately informed about the collection and sharing of their data, in breach of the UK GDPR core principle that processing should be lawful, fair and transparent: the majority of communications had been published online rather than being sent to patients directly and it was unclear how many patients had been made aware of the programme through their GP surgeries. Additional concerns centred on the measures that were being taken to secure patient data and the requirement for patients to opt out of the scheme rather than having to actively opt in.

2.2.2 Data Protection Concerns

Lack of transparency

A key concern with the proposed GPDPR was the lack of transparency in communicating to the public and GPs how the data extracting and sharing was to work. This was highlighted by the British Medical Association and the Royal College of General Practitioners and reiterated in a statement, from Elizabeth Denham, the then UK Information Commissioner (**ICO**).[4]

Although NHS Digital has said the Department of Health and Social Care and its executive agencies, NHS England, local authorities and research organisations may need to access the data, the limits on the range of other organisations which may look to access the data are unclear. "*Appropriate requests*" from organisations wishing to access the data will be scrutinised by NHS Digital's Independent Group Advising on the Release of Data and decisions will be published on NHS Digital's publicly-available Data Release Register. However, major concerns remain around access to data within the programme by "big tech" organisations who will likely see significant commercial benefits from accessing the highly sensitive information held on the database. Access to such data for research and social care purposes does not exclude data monetisation opportunities for third parties, yet data sharing restrictions seem to be weak in the face of the broad definitions of "*health and care planning and research*" purposes and the security parameters, which do not detail how to address the risks of re-identification of pseudonymised data.

It is now intended that NHS Digital will develop an engagement and communications campaign so that patients can be made aware of the scheme and in a better position to make informed choices. A DPIA reflecting the changes to the programme, and demonstrating how all risks and mitigation measures had been considered and addressed, will also be published before the data collection commences. This should help to answer many of the concerns and should go a long way in making the scheme more transparent to all.[5]

Data security

Whilst NHS Digital has said that it will be using a secure system to collect and store the data there is little information about what security measures will be in place.

Data collected as part of the scheme will be pseudonymised when it is collected from GPs. The UK GDPR defines pseudonymisation as the processing of personal data in a way that means that it can no longer be attributed to the data subject.[6] This involves replacing personal data with pseudonyms which can only be re-identified using additional information, known as a key, which must be kept separate from the pseudonymised data. NHS Digital have said that any data which could be used to identify someone directly will be replaced with unique codes and then also securely encrypted.[7]

In particular, there are concerns that NHS Digital itself could re-identify the data using other data it already holds under its existing Personal Demographics Service which contains patients' name, address, date of birth and NHS Number. Despite NHS Digital stating that data collected would not be sold or used solely for commercial purposes, there are concerns that if big tech platforms such as Google, Amazon or Apple, private health providers or insurers are able to gain access to patient data through the scheme then they may be able to use this alongside other data they hold to identify patients and exploit the data for monetary gain to the cost of the NHS.

Again, the DPIA should provide further assurance as to what risks have been identified and how NHS Digital plans to deal with those to secure patient data.

Opting out

Under the existing framework, if patients did not want their data to be shared with NHS Digital, then they were required to actively opt out rather than opting-in.

Patients can opt out of their data being shared under GPDPR by registering a Type 1 Opt-out directly with their GP surgery or a National Data Opt-out (or both). A Type 1 Opt-out prohibits the uploading and extraction of a patient's data whereas the National Data Opt-out only limits the ways that NHS Digital will be allowed to use confidential patient information for research and planning.

If patients did not opt out, then their data was designed to be automatically shared with NHS Digital when the programme went live. There was a concern that many people, especially those members of society who do not have access to the internet, may not have been able to take advantage of this opt-out.

Additionally, there was a concern that although patients could opt out after the programme had commenced, this would only prevent further data from being collected. It would not obligate NHS Digital to delete any data already collected, which by then would have been shared with multiple third parties.

The requirement now published for NHS Digital to ensure that an individual's data can be erased once they have requested to opt out of the scheme should assist in alleviating these concerns to some extent. However, given that the scheme will remain subject to patient opt-out rather than an opt-in, the requirements for valid consent under the UK GDPR will not be met and NHS Digital must therefore rely on alternative bases for the lawful collection and sharing of data.

Lawful basis

NHS Digital will only be allowed to collect and share patient data if there is an applicable lawful basis for processing data as set out in the UK GDPR. Given that, as structured, patient consent is not appropriate, it must rely on another basis under Articles 6(1) and 9(2) of the UK GDPR.

Fortunately, there were valid grounds provided in legislation: The Health and Social Care Act 2012 (the **Act**) contains provisions allowing the Secretary of State for Health and Social care (the **Secretary of State**) to make directions to instruct NHS Digital to collect and analyse data to help the health service. On 6 April 2021, the Secretary of State sent the General Practice Data for Planning and Research Directions 2021 (the **Directions**) to NHS Digital, authorising it to collect and analyse pseudonymised data from GP practices. Following receipt of the Directions, NHS Digital sent a Data Provision Notice to GP practices who were then legally required to share patient data with NHS Digital on the basis of the Directions. This notice has subsequently been withdrawn, but is likely to be replaced once the necessary conditions to restart the scheme have been satisfied, as outlined below.

Once a new Data Provision Notice has been reissued, GPs will be able to rely on Article 6(1)(c) of the UK GDPR as the lawful basis for sharing of patient data with NHS Digital as they have a legal obligation under the Act, the Directions and the Notice to share the relevant patient data.[8]

NHS Digital will also rely on this basis to collect, analyse, publish and share patient data.

The UK GDPR also states that when special categories of personal data (which include health data) are being shared, then one of the specified conditions in Article 9 UK GDPR, must also be satisfied.[9]

NHS Digital have stated that the following Article 9 conditions will be relied on:

i. Article 9(2)(g): the sharing of patient data for reasons of substantial public interest, being the processing of patient data for planning and research purposes to improve health and care services.
ii. Article 9(2)(h): the sharing of patient data for the purposes of providing care and managing health and social care systems and services.
iii. Article 9(2)(i): necessary sharing for reasons of public interest in the area of public health.
iv. Article 9(2)(j): sharing for archiving, research purposes or for statistical purposes.[10]

Next steps

Following its launch on 12 May, the original go-live date for the GPDPR data extraction was originally set as 1 July 2021. However, in view of the widespread concerns raised, it has been paused until 31 March 2022, pending satisfaction of a number of conditions, the most important in terms of data privacy being that:

- patient awareness of the scheme must be increased through a campaign of engagement and communication; and
- patients must be able to delete their personal data if they choose to opt out of sharing it with NHS Digital, even if after data has been uploaded.

Further communications from NHS Digital, since the scheme was first published, have helped to clarify and address some aspects of the concerns which have been raised but more needs to be done to ensure that the scheme is launched in compliance with data protection laws.

3 Wearables / Medical Devices

Wearable technology, also known as "wearables", is evolving to become an important category of the Internet of things, supported by the growth of mobile networks, high-speed data transfer, and miniaturised microprocessors, enabling life-changing applications in medicine and other fields. During the pandemic, there has been a rise in the use of wearables, with more people taking fitness and the monitoring of their health and wellbeing into their own hands.

Transparency

While wearables are great tools for monitoring health and general wellbeing, such devices continuously collect and store masses

of personal data, including special category health information, which, if not processed compliantly, can put data subjects at risk. Under the UK GDPR, health data falls under "special category data". In order to lawfully process special category data, a lawful basis under Article 6 and a specific condition under Article 9 of the UK GDPR must be identified. Any processing must also be fair and transparent.

Developers and owners of such devices need to ensure continued compliance with their data protection obligations, including ensuring that users are fully informed of what data is collected and how this is to be used and shared, and users should take the time to understand what is happening to their personal data by reading the privacy information provided.

Lawful grounds for processing

Where the personal data of an average user is to be uploaded and processed through the app of the wearable device, the legal basis for processing any special category data is likely to be explicit consent. Consent may also be required to process user personal data not deemed sensitive.

However, other personal information, such as GPS location or contact details, may be justified on the grounds of contract or legitimate interest. The provider's privacy notice will need to be accessible to the individual at the time the data is collected. It will need to include an explanation of the data collected, and the lawful grounds for processing. For consent to be valid under the GDPR it must be freely given, specific to the use it is collected for, and be clear and unambiguous. It will need to ensure not only that users can easily withdraw consent but also that their personal data is not further processed. If explicit consent is required in relation to the processing of special category data, it must be provided separately in a clear and specific statement, and cannot be inferred from an individual's conduct.

The position is more complicated, however, where a sports club or coach is looking to use a smart wearable device to analyse performance data of its professional athletes, including where this is built into a smart kit that the athlete is required to wear. Where this is done in the context of an employment relationship, consent is unlikely to be the appropriate basis as it is unlikely to be deemed "freely given" by the athlete. Other lawful bases that may be available include those under Article 9(2)(b) or 9(2)(h) UK GDPR but, in the latter case, would require any processing to be carried out by or under the supervision of any appropriate health professional.

Privacy and Security by Design

The UK GDPR requires health tech companies to implement – from the outset – appropriate technical and organisation measures to ensure the protection of individual rights. This approach means that developers will need to incorporate UK GDPR-compliant processes at every step of the way, from the design phase of a system, service or product throughout its entire life cycle. All the UK GDPR principles will apply to that effect:

- data minimisation means that the app may only collect and process the minimum amount of data necessary to achieve the specific purpose (which must be clearly set out);
- data security means that personal data must be processed in a manner that ensures appropriate security of the personal data;
- purpose limitation on the use of data means that personal data may only be processed by the app for the purpose for which the personal data was collected;
- data Retention means that personal data should not be stored for longer than necessary; and
- accuracy of data means that personal data must be kept up to date.

As the app provider must be able to demonstrate compliance with the principles set out in the UK GDPR, conducting a DPIA will assist with this objective and remains the best practice in any case when it comes to health and wellness apps, where there is a likelihood of high risk to the individual, A DPIA will be able to assess three main considerations: (1) definition of the nature and scope of the data collected; (2) determination of the necessity and compliance measures required; and (3) identification of the risks to individuals, together with the appropriate measures to mitigate those risks.

4 Looking Forward: Data Protection Reforms

The ICO and the UK Government's Department for Digital, Culture, Media and Sport (**DCMS**) have launched a number of consultations impacting data protection and data security rules applicable to digital health.

4.1 ICO consultation on data transfers

The ICO launched a consultation on 11 August 2021 on "how organisations can continue to protect people's personal data when it's transferred outside of the UK". The ICO consultation includes a three-part data transfer suite of proposals and options as follows:

- Proposal and plans for updates to guidance on international transfers.
- Transfer risk assessments.
- The international data transfer agreement.

At this time, the outcome of the consultation has not yet been published but it will have a significant impact on the digital health sector as the proposals aim to facilitate the flow of data to non-adequate jurisdictions while maintaining high standards of data protection for people's personal information when being transferred outside of the UK.

4.2 DCMS Consultation "Data: A New Direction"

On 10 September 2021, the UK DCMS launched a consultation outlining its proposals to extensively reform the UK's data protection and privacy regime, "Data: A new Direction" (https://www.gov.uk/government/consultations/data-a-new-direction), following its departure from the EU. A year after the publication of the National Data Strategy,[11] the Consultation further explores the potential for new data rules to better support the digital economy, establish a pro-growth and innovation friendly regime across the UK, increase trade and improve healthcare while maintaining high data protection standards. The objectives set out in this paper are consistent with the proposals put forward by the UK government at the G7 summit roundtable of Data Protection and Privacy Authorities[12] held on 7 and 8 September 2021, in relation to the design of artificial intelligence in line with data protection.

The Consultation sets out in five chapters the areas of focus for data protection reform including:

- Chapter 1 – Reducing barriers to responsible innovation.
- Chapter 2 – Reducing burdens on businesses and delivering better outcomes for people.
- Chapter 3 – Boosting trade and reducing barriers to data flows.
- Chapter 4 – Delivering better public services.
- Chapter 5 – Reform of the Information Commissioner's Office.

In particular, the consultation outlines several proposals for amendments to research provisions within the existing data

protection framework with a view to ensure legal certainty and reduce complexity for organisations that process personal data for research. It notably proposes to establish a statutory definition for "scientific research" and create a new separate lawful ground for research. It aims to simplify the rules on using (and re-using) data for research.

The consultation also aims to address the complexity of the governance rules applicable to AI, Machine Learning and the use of AI technology. Unlocking the power of data is one of the government's top 10 technology priorities. The National AI Strategy published on 22 September 2021 underscores the importance of this consultation and the role of data protection for broader AI governance. The consultation asks for views on whether organisations should be permitted: "to use personal data more freely, subject to appropriate safeguards, for the purpose of training and testing AI responsibly."

A source of much debate is the proposal that Article 22 of the UK GDPR, which provides that individuals must not be subject to solely automated decisions which produce legal effects or similarly significant effects, without human intervention, should be removed and solely automated decision making permitted.

The government supports the use of "data intermediaries", which may well be the role for which many health-tech providers qualify, and aims to champion data intermediary activities such as data sharing, processing and pooling to "ensure responsible and trusted data use".

Finally, obstacles to international data flows have been identified as a main concern to efforts of international data sharing and research during the pandemic. The DCMS proposal includes plans to agree a series of post-Brexit "data adequacy" partnerships with the United States, Australia, the Republic of Korea, Singapore, the Dubai International Financial Centre and Colombia. The UK will also prioritise future partnerships with India, Brazil, Kenya and Indonesia. The "data adequacy" partnerships are formed with countries deemed to have high data protection standards and mean organisations do not have to implement additional compliance measures to share personal data internationally. A Mission Statement on the UK's approach to international data transfers and the "UK Adequacy Manual" were also published on the same day the consultation was published.

5 Conclusion

The ongoing nature of the COVID-19 pandemic means that the use of data for healthcare purposes such as contact tracing, medical research and public policy development is likely to continue. The use of data will continue to play a vital role in assisting and shaping the response to the challenges that the virus poses. To facilitate this use of data, individuals must have trust and confidence that their data will be processed in accordance with data protection rules, securely, fairly and transparently and developers, healthcare bodies and government must pay to embed data protections in their innovation processes at all stages.

Acknowledgment

The authors are grateful for the contributions made to this chapter by Gareth Bell, trainee solicitor within the Data/Commercial Team.

Endnotes

1. Blog: *Regulating Through a Pandemic*: J. Dipple-Johnston, Deputy Commissioner and Chief Regulatory Officer, ICO, 27 July 2021.
2. ICO, *COVID-19 Contact tracing: data protection expectations on app development*, 4 May 2020.
3. ICO, *ICO takes action against contact tracing QR code provider*, 18 May 2021.
4. ICO, *Elizabeth Denham Statement on Delay to the Launch of GPDPR*, 8 June 2021.
5. Jo Churchill, *Letter from Jo Churchill MP*, 19 July 2021.
6. Article 4(5) UK GDPR.
7. NHS Digital, *Collecting GP Data – advice for the public*, 24 August 2021.
8. Article 6(1)(c) UK GDPR.
9. Article 9 UK GDPR.
10. NHS Digital, *General Practice Data for Planning and Research: GP Practice Privacy Notice*, 24 August 2021.
11. https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy.
12. https://ico.org.uk/media/about-the-ico/documents/4018242/g7-attachment-202109.pdf.

Dr. Nathalie Moreno is a Data Protection and Cyber Security Partner at Addleshaw Goddard's London and Paris offices. She is a well-known and trusted adviser in the global privacy and data protection world, who brings 20 years of experience and extensive knowledge to European and global clients with a particular focus on the technology, healthcare and life sciences sectors. Nathalie's practice encompasses the full range of Data Protection, e-Privacy and Cyber Security issues including advisory, public policy advice to regulators and governments, transactional and pre-contentious advice in the areas of life sciences (pharma, biotech and medical devices) as well as health technology, technology-enabled healthcare, digital health services and mobile health (powered by AI, IoT and IoMT).

Addleshaw Goddard LLP
Milton Gate, 60 Chiswell Street
London, EC1Y 4AG
United Kingdom

Tel: +44 20 7160 3179
Email: Nathalie.Moreno@addleshawgoddard.com
URL: www.addleshawgoddard.com

Johanna Saunders is a seasoned commercial lawyer with a background in company law and experience as an accredited Practitioner in Data Protection and Certified Information Privacy Professional (Europe). Jo has experience advising organisations on data and IT contracts, international data transfers, Article 30 records and cybersecurity in health and retail sectors. Specialising in data and IT law, she can support and advise major organisations on information matters, including processing arrangements, cross-border data transfers, privacy and retention policies, data subject access requests and management of cyber incidents. She also advises on pharmacy regulation and commercial contracts more generally.

Addleshaw Goddard
One St Peter's Square
Manchester, M2 3DE
United Kingdom

Tel: +44 161 934 6572
Email: Johanna.Saunders@addleshawgoddard.com
URL: www.addleshawgoddard.com

Annabelle Gold-Caution is an experienced Privacy and Technology lawyer based in Manchester. She advises organisations on strategic tech, cybersecurity and data-driven issues in the health, digital and retail sectors. She provides a full complement of support and advice to businesses on privacy compliance, in particular advising on interactions with regulators, building cross-functional data protection compliance programmes and on large-scale, complex cybersecurity incidents and technology projects in time-pressured conditions. Her recent experience includes advising an international healthcare provider on cross-border sharing of patient data for research purposes, including for collaborative initiatives using AI to identify medical insights. She regularly publishes articles on topical privacy issues and speaks at industry conferences.

Addleshaw Goddard LLP
One St Peter's Square
Manchester, M2 3DE
United Kingdom

Tel: +44 161 934 6126
Email: Annabelle.Gold-Caution@addleshawgoddard.com
URL: www.addleshawgoddard.com

Lydia Loxham is a Commercial and Privacy lawyer based in Manchester. She advises organisations on a range of commercial contract, cybersecurity and data issues in the digital, retail and consumer sectors. She is experienced in advising on, negotiating and drafting agreements for the provision of goods and services, distribution agreements and consumer terms. Her recent experience includes advising global service providers in relation to cross-border data transfers and advising businesses in the retail and consumer sector in relation to data protection and consumer law compliance.

Addleshaw Goddard LLP
One St Peter's Square
Manchester, M2 3DE
United Kingdom

Tel: +44 161 934 6202
Email: Lydia.Loxham@addleshawgoddard.com
URL: www.addleshawgoddard.com

Austria

Herbst Kinsky Rechtsanwälte GmbH

Dr. Sonja Hebenstreit

1 Digital Health

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 Austrian Federal Ministry of Health's definition (see https://www.sozialministerium.at/Themen/Gesundheit/eHealth.html) uses the term "e-health" as the general term, comprising the use of information and communication technologies in health-related products, services (including telemedicine) and processes. The Ministry uses the term "telemedicine" as referring to the provision or support of healthcare services using information and communication technologies, where the patient and the healthcare provider are not present in the same place. This is in line with the definition used by the European Commission who 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 digital health technologies in your jurisdiction?

Key emerging technologies are, in particular, artificial intelligence (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 digital health for your jurisdiction?

The core legal issues in digital health are: compliance with data protection (see sections 4 and 5); the technical requirements (see *GTelG 2012* in question 2.2); as well as the determination of whether a product qualifies as a medical device (see questions 2.1 and 3.1).

1.4 What is the digital health market size for your jurisdiction?

There is no reliable data available regarding the digital health market size for Austria, as the available statistics either do not refer to Austria in particular or only consider specific segments of the total digital health market.

According to a market outlook as published by Statista (see https://de.statista.com/outlook/dmo/digital-health/oesterreich?currency=EUR), the overall revenue for 2021 in Austria in the e-health sector amounts to approximately 227.60 million euros. However, this survey does not take into account the public e-health sector in Austria (which is the most relevant sector) as it only includes non-prescription e-health devices and apps.

In another study recently published by Roland Berger (see https://de.statista.com/statistik/daten/studie/1178751/umfrage/umsatz-auf-dem-markt-fuer-digital-health-weltweit/), the volume of the digital health market in 2026 in Germany was estimated to 59 billion euros. Consequently, one tenth of this (5.9 billion euros) could be assumed for Austria's digital health market volume in 2026 as a tentative estimate (due to the size ratio between Austria and Germany).

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

As pointed out in question 1.4, there are no reliable figures available on the Austrian digital health market size for Austria. Therefore, we can therefore not provide an overview of the five largest digital health companies by revenue.

Further, please note that a major part of digital health solutions applied in Austria is organised by the Austrian state (e.g. "ELGA") and implemented by the Umbrella Association of Austrian Social Insurance Institutions.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The Austrian Physicians Act 1998, Federal Law Gazette I 169/1998, as last amended by the Federal Law Gazette I 172/2021, (*Ärztegesetz* 1998, *ÄrzteG* 1998) contains, in principle, 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 a distance, without direct human contact. The Austrian Medical Association has stated that telemedicine might support the relationship 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), whereas in the case of telemedicine, they need to be in full control of the patient's situation, and the telehealth 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 23/2020, (*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 122/2021, (*Medizinproduktegesetz*, *MPG*) as well as the Medical Device Regulation 2017/745 on medical devices (MDR), which entered into force on May 26, 2021, after having been postponed for a year due to the COVID-19 pandemic, constitutes the major regulatory framework for medical devices. 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 core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The General Data Protection Regulation, Regulation 2016/679 (GDPR) contains central provisions on data protection. Although the GDPR as a regulation applies uniformly and directly throughout the European Union, a large number of opening clauses allow national deviations by Member States. Providers of digital health 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, Federal Law Gazette I 111/2012 as last amended by Federal Law Gazette I 34/2021, (*Gesundheits-Telematikgesetz* 2012, *GTelG 2012*) contains special regulations for the electronic processing of health data and genetic data (please refer to Article 4 Nos 13 and 15 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 Umbrella Association of Austrian Social Insurance Institutions and the federal provinces or their health funds. In the context of *ELGA*, other e-health services have been introduced as well such as the electronic medication prescription (e-medication) or the electronic vaccination pass ("e-vaccination pass"; see section 24b *et seq. GTelG 2012* as well as eHealth Regulation, Federal Law Gazette II 449/2020, last amended by Federal Law Gazette II 112/2021).

To meet the challenges of the COVID-19 pandemic, (temporary) simplifications to the conditions of transmitting health data via email and fax for healthcare providers have been implemented to the *GTelG* as well.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The Medical Devices Act and, since May 2021, the Medical Devices Regulation (see question 2.1) likewise apply to Consumer Devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

In connection with *GTelG 2012* and *GTelV 2013*, Federal Law Gazette II 506/2013 (*Gesundheitstelematikverordnung*) 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?

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.

In 2018, the *DSB* 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 it is 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 lifestyle 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.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

The terms "Artificial Intelligence" (AI) or "Machine Learning" (ML) are generic and rather technology neutral terms, as they represent a wide range of different kinds of technologies. To date, there is no definitive legal definition available in the Austrian or European jurisdiction (although the European legislator has increasingly dealt with these topics, as for example in its draft for an AI Regulation 2021/0106 (COD), albeit on a rather technology neutral level). *De lege lata*, the same regulations apply to AI or ML as to all other technologies, for the healthcare sector, in particular, the MDR as well as the GDPR.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  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 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 fears 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 telemedicine or virtual care services in general, but a specific regulation has been issued regarding the provision of teleradiology services: the Medical Radiation Protection Regulation, Federal Law Gazette II 375/2017 (*Medizinische Strahlenschutzverordnung*) 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.
  The COVID-19 pandemic has led to a massive increase regarding the use and offer of telemedicine services.
  As outlined above (question 2.2), due to the COVID-19 pandemic, (temporary) simplifications to the conditions of transmitting health data (via email and fax) for healthcare providers have been implemented to the *GTelG*.
- **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.
- **Clinical Decision Support Software**
  See question 2.6. Further, the GDPR, in particular its provisions on automated individual decision-making (Article 22 GDPR), needs to be considered in case personal data is processed.
- **AI/ML powered digital health solutions**
  See question 2.6 (Software as a Medical Device) and section 8 (AI and Machine Learning).
- **IoT and Connected Devices**
  "Internet of Things" (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); furthermore, the GDPR needs to be considered in case personal data is processed.
- **3D Printing/Bioprinting**
  Bioprinting raises a wide range of legal and ethical questions. Currently, no *sui generis* regulatory regime governing the entire bioprinting process is in place in Austria. According to the European Commission and the European Medicines Agency, tissue engineered products might fall under the definition of advanced therapy medicinal products (ATMPs). Additionally, IP and, in particular, patent rights questions might arise.
- **Digital Therapeutics**
  Digital Therapeutics is a rather broad term used for device-controlled therapy measures. In particular, digital therapeutics may be subject to the MDR as well as provisions of the GDPR. In view of its high-risk potential, digital therapeutic software shall, according to Annex VIII; Rule 11 of the MDR, be classified as a medical device of at least risk class IIa.
- **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; furthermore, the GDPR needs to be observed.

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.

Digital platforms must take appropriately (high) technical/organisational measures for data security when processing health data (Article 32 GDPR) and the *GTelG 2012* needs to be considered in case personal health data is processed.

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 personal 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).

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 personal 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, namely the principles of transparency, lawfulness, purpose limitation, data minimisation, proportionality, accuracy, data security and accountability. As in the context of digital health services, large scale processing of sensitive personal data will be involved, the entity providing such services is required to designate a Data Protection Officer in accordance with Article 37 para 1 lit c GDPR. Furthermore, a data protection impact assessment (DPIA) might be required (e.g., according to Article 35 para 3 lit b GDPR) before processing is started.

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). Neither the GDPR nor the *DSG* contain regulations defining the scope of data use in the context of digital health.

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/data subject. 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. In the event where more than one controller jointly decides on the respective processing, an agreement on joint controllership needs to be concluded between these controllers.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The key legal issues and therefore greatest challenge with regard to securing comprehensive rights to personal data is that the personal data must be collected in accordance with the principles pursuant to Art 5 GDPR and that a corresponding legal basis must be guaranteed for each processing at all times. Successfully facing those legal issues is not only important because of the severe penalties for the unlawful processing of personal data provided for in the GDPR (Article 83 GDPR); it is also vital for any digital (health) application using personal data to safeguard that such use is lawful as otherwise the application risks being shut down by the data protection authority at any time.

However, the GDPR is only applicable to personal data. Therefore, if no personal data according to Article 6 or Article 9 GDPR is processed, a specific right to process the data is not necessary from a data protection point of view.

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, the *GTelG 2012* does not apply.

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

Please refer to question 4.3 and 5.1.

6 Intellectual Property

6.1 What is the scope of patent protection?

Technical inventions that 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, Federal Law Gazette I. No. 259/1970, as last amended by Federal Law Gazette. I No. 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.

Software programs as such cannot be subject to patent protection.

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 I 111/1936 as last amended by Federal Law Gazette I 105/2018 – *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 Unfair Competition Act, Federal Gazette I 448/1984, as last amended by Federal Gazette I 104/2019 (*Bundesgesetz gegen unlauteren Wettbewerb*, *UWG*) contains in its Sections 26a *et seq.* 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.

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 rules or laws that apply to academic technology transfers in your jurisdiction?

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, Federal Gazette I 120/2002, as last amended by Federal Gazette I 177/2021, (*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 as such will be protected by copyright law; whether patent protection can be sought needs to be assessed individually.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

Exclusively natural persons can be named and registered as an inventor for patents, as the legal institution of an "e-person" is not recognised in Austrian law. If an AI-device should "invent" a patentable product, this goes back to the actual inventor (natural person) of the AI device.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

In principle, the rules of the Patent Act regarding service inventions (section 7 *et seq.* Patent Act) apply to inventions made within academic (see question 6.4), or other public-funded institutions (see e.g. Federal Act on General Matters Pursuant to Article 89 of the GDPR and the Research Organization (*Forschungsorganisationsgesetz – FOG*), Federal Law Gazette I 341/1981, as amended by Federal Law Gazette I 75/2020, and Federal Act on the Institute of Science and Technology Austria (*IST-Austria-Gesetz – ISTAG*), Federal Law Gazette I 31/2018, as amended by Federal Law Gazette I 75/2020).

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 healthcare and non-healthcare companies?

Besides regulatory considerations (see 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). For using such data, a licence agreement needs to be concluded with the respective right holder.

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 requires 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 solutions?

No specific liability schemes for adverse outcomes in digital health solutions exist under Austrian law. 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 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 of any cross-border provision of digital health services, the respectively applicable law and the applicability of regulatory requirements have to be determined.

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, practice 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-healthcare companies should consider before entering today's digital healthcare 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 healthcare 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.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

One key barrier is Section 3 *ÄrzteG* according to which medical advice may only be given by licensed physicians. Furthermore, the funding and/or (non-)reimbursement of digital health solutions by the state sick funds is a major issue and might be a barrier to the widespread use of digital health solutions.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

From a formal/legal point of view, under Austrian law, clinician certification bodies might not be of specific relevance, even though acceptance or endorsement of a specific digital health solution by such body might prove compliance with specific quality standards or recommendations issued by such body. However, within a possible legislative process, these bodies might typically be consulted. The introduction of digital health solutions is in principle exclusively governed by law.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

The Austrian state provides for a central digital health solution, namely "ELGA" (see question 2.2), which is owned by the Republic of Austria, the Umbrella Association of Austrian Social Insurance Institutions as well as the federal provinces or their health funds. The services that are provided within ELGA (e.g. e-medication) do not have to be paid separately by patients and are covered by the general health insurance. The legal requirements of ELGA are set forth in the *GTelG 2012*.

Any other digital health solution an individual might want to use would need to be prescribed by a physician and be appropriate in order to be reimbursable by the Austrian Social Insurance Institutions.

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. Hebenstreit represents Austrian and international clients, including numerous pharmaceutical and medical devices companies, in a variety of regulatory issues, licensing and other contractual matters as well as in data protection, unfair competition and reimbursement matters.

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. The Firm has established a particularly strong presence in the field of Life Sciences and Healthcare.

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

Belgium


Olivier Van Obberghen


Pieter Wyckmans


Amber Cockx


Wietse Vanpoucke

Quinz

1 Digital Health

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

While more than one definition exists, digital health or e-health is generally described as "the use of information and communication technologies within healthcare to optimize patient care".

1.2 What are the key emerging digital health technologies in your jurisdiction?

In recent years, Belgium has seen a rise in the development and implementation of a number of health technologies such as apps, wearables, platform technology and AI-based software across the life sciences value chain and into the patient journey with a focus on remote, personalised, precision and preventative care.

1.3 What are the core legal issues in digital health for your jurisdiction?

The emergence of new health technologies results in changing roles for healthcare actors and challenges the boundaries of the current legal framework. With an increasingly consumer-centric approach to healthcare, patients are empowered to take an active role in the co-maintenance of their own health. In response, the role of the hospital is gradually shifting from a focus on inpatient to outpatient treatment, while the medical (tech) industry more often comes into direct contact with patients, leading to data protection and compliance concerns. The reality of an ever-increasing digitalisation of healthcare is often at odds with existing laws and regulations (concerning, for example: intellectual property protection; data protection; liability; and compliance) and will continue to require swift and agile action by the legislator.

1.4 What is the digital health market size for your jurisdiction?

There are currently no official statistics available that provide a clear overview of the size of the Belgian digital health market. This is mainly due to the broadness of the concept of digital health and the difficulty of delineating its boundaries.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

In line with question 1.4, no definite statistics on Belgium's largest digital health companies exist. Belgium's digital health landscape is populated by multinational (tech) corporations headquartered abroad, biotech and pharmaceutical companies venturing into digital branches and a large number of fast-growing start-ups, scale-ups and spin-offs.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Some of the core healthcare regulatory schemes are as follows:

- Act on the Performance of the Healthcare Professions of 10 May 2015;
- Act on Hospitals and Other Care Facilities of 10 July 2008;
- Health Care Quality of Practice Act of 22 April 2019 (applicability postponed to July 1, 2022);
- Patients' Rights Act of 22 August 2002;
- Law on Medicines of 25 March 1964;
- EU Regulation 2017/745 on Medical Devices; Medical Devices Act of 22 December 2020; EU Regulation 2017/746 on *in vitro* diagnostic medical devices of 5 April 2017 (applicable as of 26 May 2022);
- Law on Experiments with Humans of 7 May 2004;
- Law on clinical trials with medicines for human use of 7 May 2017; and
- EU Regulation 536/2014 on clinical trials on medicinal products for human use of 16 April 2014 (applicable as of 31 January 2022).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The legislation on product safety, personal data protection and e-commerce apply to digital health and healthcare IT. In addition, general regulations on competition, consumer law and unfair commercial practices must be kept in mind. Certain specific rules might also be relevant, e.g. the Act of 21 August 2008 establishing and organising the eHealth platform or the

EU framework on cross-border healthcare. Lastly, a number of substantial legislative proposals in light of the EU's digital strategy (i.e. regarding digital services, markets, content, artificial intelligence, cybersecurity, etc.) will significantly impact the offering of digital health goods and services in the future.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The legislation on medical devices (see question 2.6), product liability (see question 9.1), e-commerce and the consumer protections set forth in the Code of Economic Law (CEL), Book VI are relevant to consumer healthcare devices. Intellectual property rights of software are protected by Book XI, Title 6 of the CEL.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? 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. Additionally, professional associations such as the Order of Physicians and the Order of Pharmacists regulate the deontological aspects of healthcare professions, while the self-regulatory organisation Pharma.be provides industry guidance. Lastly, the Belgian Data Protection Authority (DPA) enforces compliance with data protection.

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

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. Lastly, the EU Commission and the Belgian Competition Authority implement the competition policy on the Belgian 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) or an accessory to a medical device, the Medical Devices Act of 22 December 2020, the EU Regulation 2017/745 on Medical Devices (MDR) and/or the EU Regulation 2017/746 on *In Vitro* Diagnostic Medical Devices (applicable as of 26 May 2022) (IVDMDR) will apply, depending on the type of medical device. Prior to being placed on the market, medical devices must undergo a clinical evaluation and conformity assessment to review the safety and performance of the device. In addition, medical devices need to be traceable throughout the supply chain up until the end user. Finally, the FAHMP is responsible for post-market surveillance of (software as a) medical device.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

Software that is powered by Artificial Intelligence (AI)/ Machine Learning (ML) is currently governed by the same regime as other software (see questions 2.3 and 2.6). If AI/ML powered digital health devices or software solutions fall within the scope of the MDR or the IVMDR, they must thus be CE-marked (after having completed a successful conformity assessment) before being placed on the market. It can, however, be expected that AI/ML powered devices or software will in the future be regulated by specific instruments. In this regard, the European Commission has proposed new draft regulation on artificial intelligence (the AIR). The AIR recognises that, if AI/ML powered digital health devices or software solutions constitute medical devices, they may be identified as high-risk, and both the requirements of the MDR/IVMDR and the AIR will have to be complied with.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  A comprehensive regulatory and reimbursement framework for healthcare provided at a distance is currently still lacking in Belgium. Up until recently, the National Council of the Order of Physicians (NCOP) argued that the diagnosis of patients without the presence of both the physician and the patient in the same place posed risks and telemedicine with the aim to diagnose a patient would only be justifiable in exceptional cases. On the other hand, telemonitoring or tele-expertise between physicians where no diagnosis was made could be performed at a distance. In addition, telemedicine was not part of the nomenclature of NIHDI and therefore not reimbursed. The COVID-19 crisis, however, forced a breakthrough with regard to healthcare services provided at a distance. Under the emergency measures taken by the legislator and the government to contain the virus, telehealth services performed under certain conditions were allowed and reimbursed by the NIHDI. Although these measures are of a temporary nature, it can be expected that the widespread switch to telehealth services during the pandemic will accelerate the adoption of a more definitive legal framework governing the conditions and reimbursement of telemedicine. Proof of transforming attitudes *vis-à-vis* virtual care can already be found in a few recent telehealth initiatives that received the approval of both the NCOP and the NIHDI.
- **Robotics**
  Although the traditional rules regarding (contractual, extracontractual, medical and product) liability apply (see question 9.1 below), it may be difficult for a patient suffering damage due to robot-assisted surgery to assess the most suitable remedy for her/his claim and the current EU and national liability framework may prove to be inadequate.
- **Wearables**
  Wearables are subject to considerably different regulatory frameworks based on their classification as a medical device or not. The decisive criteria to determine whether a wearable constitutes a medical device, is to establish whether the instrument, appliance or software is intended to be used for one of the medical purposes in art. 2(1) of the MDR (e.g. for the diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of a disease or disability). The medical devices framework is relatively burdensome, giving manufacturers an incentive to indicate that their health product is not intended to be used for one of these medical purposes in order to avoid having to

comply with the MDR. On the other hand, reimbursement for wearables is currently limited to CE-certified medical devices (see further under "*Mobile Apps*"). Consequently, manufacturers must carefully assess whether a wearable should be considered a medical device during product development and in determining a market access strategy, as this decision will result in disparate regulatory pathways.

- **Virtual Assistants (e.g. Alexa)**
  Virtual (voice) assistants (VVAs) have ample applications in healthcare settings. They can aid in clinical notetaking, in assisting an aging population or patients suffering from mobility issues, in medication management and in health information seeking activities. However, data protection and privacy concerns have been raised by (amongst others) the European Data Protection Board in its Guidelines 02/2021 on virtual voice assistants. Careful consideration must be given to the legal basis of the processing of personal data by virtual assistants under art. 6 of the General Data Protection Regulation (GDPR) and the requirements of art. 5(3) of the Directive 2002/58/EC on privacy and electronic communications (as transposed into Belgian law by the Electronic Communications Act of 13 June 2005). Since virtual voice assistants require processing of biometric data for user identification, an exemption under art. 9 of the GDPR must also be sought. Other data protection challenges have also been raised, for example regarding the data minimisation principle and the accidental collection of personal data or the collection of background noise or other individuals' voices besides the user. The European Commission has also voiced antitrust concerns about virtual assistants in light of its consumer Internet of Things (IoT) inquiry. These concerns included the high entry and expansion barriers of the technology, certain exclusivity and tying issues, the lack of interoperability, the large amounts of data feeding into the technology and VVAs functioning as intermediaries between the user and smart devices or IoT services.
- **Mobile Apps**
  Since January 2021, mobile apps can be reimbursed if they fulfil all criteria of the mHealth Belgium validation pyramid. In the first instance, they need to be CE-certified as a medical device and meet the requirements of the GDPR. Secondly, they need to pass certain interoperability and connectivity criteria. Lastly, a socio-economic benefit must be demonstrated in order to receive reimbursement by the NIHDI. However, some other issues concerning mobile apps remain. For example, if mobile health apps are used in healthcare and prescribed by a healthcare professional, patients do not have access to the Internet may not be discriminated and the patient's rights under the Patients' Rights Act need to be respected, such as the right to quality healthcare. Again, mobile apps may be classified as a medical device if intended to be used for medical purposes and may consequently have to comply with the medical devices' framework, while other apps may be considered a wellness or lifestyle device.
- **Software as a Medical Device**
  The classification of Software as a Medical Device (SaMD) suffers from the same shortcomings as the ones for wearables and mobile apps. Software will be considered a medical device if: (i) 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; (ii) it performs an action on data that goes beyond storage, archival, communication or simple search; and (iii) it is for the benefit of individual patients. As said, classification as a medical device has consequences for the regulatory framework that applies to software.
- **Clinical Decision Support Software**
  Besides the undeniable ethical challenges**,** clinical decision support software (CDSS) raises a number of legal issues. It is, for example, uncertain which party will be responsible in the event of a medical accident as a result of a decision made on the basis of CDSS. In addition, there are data protection and medical confidentiality concerns, for instance if the patient data that is submitted to the CDSS is used, not only to render a medical decision concerning the relevant patient, but also to improve the CDSS or for other business purposes of the CDSS manufacturer. As further set out below, due to the requirements of the GDPR in relation to automatic decision-making, human intervention by a healthcare professional before making a final medical decision is in any case advised.
- **AI/ML powered digital health solutions**
  A key barrier in the widespread implementation of AI/ML powered solutions in healthcare concerns the massive amounts of special category personal data that are often needed for the optimal functioning of these devices and the accompanying data protection aspects, for example in relation to automated decision-making by AI/ML powered solutions. According to art. 22 of the GDPR, a data subject is entitled not to be subject to a decision based solely on automatic means that significantly affects them. While there are exceptions to this principle (e.g. explicit consent and suitable safeguards), a data subject has the right to receive meaningful information about the logic involved in the automatic decision-making and to obtain human intervention and contest a decision made by automated means. This is particularly difficult when the processing has been done by artificial neural networks, as it may be impossible to determine how the AI decided on a particular outcome. Exercising other rights, such as the right to access and erase personal data might (technically) also be notably difficult. Besides data protection, the interplay of the proposal AIR and the MDR suggests that AI-powered medical devices will in the future be regulated by stringent requirements in both instruments. Any AI-powered medical device that must undergo a conformity assessment procedure by a notified body is considered as a high-risk AI-system within the meaning of the AIR (art. 6 and Annex II of the AIR), subject to strict monitoring obligations. Since most software as a medical device will be classified as Class IIA or higher and must therefore undergo a conformity assessment, the majority of AI/ML powered medical devices will be deemed to be high risk under the AIR.
- **IoT and Connected Devices**
  Again, while 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.
- **3D Printing/Bioprinting**
  Legal considerations on bioprinting include IP questions (copyright, patentability and design rights of techniques and materials), the classification of the bioprinted product (as medical device or (advanced therapy) medicinal product) and the liability of the variety of actors involved.
- **Digital Therapeutics**
  Digital therapeutics (DTx) have great potential in shifting healthcare to be more personalised, preventative and patient-centred. The downside, however, includes major concerns relating to cybersecurity, data protection and privacy. By using digital implements such as mobile

devices, sensors and IoT, DTx transfers enormous amounts of personal information over the Internet and hence, risks of unauthorised access and manipulation of these products and underlying data (e.g. further use of real-world evidence) could compromise both trust in the product and patient care. Since some of the key therapeutic areas of digital therapeutics include cognitive behavioural therapy and lifestyle management (e.g. for patients with chronic conditions), it may be especially difficult to distinguish whether a DTx solution is a medical device or not.

- **Natural Language Processing**
  Natural language processing technology is similarly impacted by data protection concerns as virtual assistants are (see above). Healthcare professionals wishing to use this technology in the management of electronic health records may also encounter interoperability issues.

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).

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 few 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 "sensitive personal data" or a "special category of personal data". In principle, such data cannot be processed unless a valid legal basis can be found and 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. (arts 6 and 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 the 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 under the penalty of criminal sanctions in accordance with art. 458 of the Criminal Code (art. 25 Code of Medical Ethics of the NCOP). 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 (arts 9.2(h) and 9.3 GDPR). Accordingly, health app providers cannot benefit from this provision and will have to rely on any of the other exceptions in art. 9 (e.g. freely given, specific and informed consent (art. 9.2(a)), where processing is necessary for reasons of public interest in the area of public health (art. 9.2(i)) or where processing is necessary for scientific research purposes (art. 9.2(j)).

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, arts 22–24 Code of Medical Ethics of the NCOP, arts 33–40 of the Health Care Quality of Practice Act of 22 April 2019). 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.

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 nearly any action or operation related to 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 arts 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?

When more than one party is involved in the processing of (health-related) personal information, both territorial aspects and the relationship between the parties need to be considered. On the one hand, 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 located in the EU (if related to the offering of goods and services or the monitoring of behaviour of data subjects within the EU). If personal data that is subject to the GDPR is transferred to a controller or processor outside the EEA (not normally subject to the GDPR), a transfer mechanism (such as the newly adopted standard contractual clauses) needs to be implemented and a transfer impact assessment may be necessary. On the other hand, it is essential to allocate the rights and responsibilities of each actor involved in the processing. Whenever a processor processes data on behalf of a controller, a data processing agreement must be concluded (art. 28.3 GDPR). This is the case if a physician makes use of a medical device for the diagnosis of her/his patients and personal data will be processed by the medical device provider for such healthcare purposes. If such provider also processes personal data for its own purposes and means (e.g. to improve its products and services), such provider may – in addition – be considered a controller, for which the GDPR does not require a specific agreement. Further, if the physician and medical device provider jointly determine the purposes and means of the processing and thus relate to each other as joint controllers, the parties must conclude a transparency agreement (art. 26 GDPR).

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The GDPR maintains a purpose limitation principle, meaning that personal data that is collected for a certain purpose cannot be used for a new and incompatible purpose (art. 5.1(b) GDPR). It is thus important to establish all purposes for which the personal data will be used at the time of collection. This is particularly relevant in the context of clinical trials. All too often, personal data collected in the course of a clinical trial (first use) may become of interest for the use in other research, independent of this clinical trial (secondary use). The purpose limitation principle prohibits further processing of personal data incompatible with the initial purpose, however, further processing in accordance with art. 89(1) of the GDPR for scientific research purposes shall not be considered incompatible with the initial purpose. Nonetheless, if the legal basis for the further processing of personal data (secondary use) is consent under art. 6.1(a) of the GDPR, this may pose certain problems. Consent must be freely given, specific, informed and unambiguous. However, often at the beginning of the clinical trial (first use) when consent of the data subject is sought, it is not yet entirely clear for which further research purposes the personal data may also be used (secondary use). Fortunately, recital 33 of the GDPR allows for some flexibility in this regard and notes that data subjects should be permitted to give their consent for the secondary use of their personal data for scientific research on a more general level. Ensuring that data subjects give their consent at the time of collection for all purposes for which one intends to use the personal data is good practice and avoids the situation where one would have to go back to the data subject to ask for consent for additional purposes.

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 (if the legal basis for the processing of personal data is consent). In an information society, the obligation to professional secrecy no longer suffices to protect a patient's medical data. In this context, it is highly recommended to enter into a data sharing agreement addressing what data can be shared, who has the authority to access the data and which security measures are required, especially when there is a large number of parties involved in the processing of personal data. These considerations are also at the forefront in the European Commission's proposal of a European Health Data Space.

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

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 another aspect of the processing of data under Belgian law. Correspondingly, the same regulatory requirements apply (see question 4.3). Notably, a data subject must be informed about the third parties with whom its personal data will be shared. Further, if the third party is situated outside the scope of the GDPR, adequate safeguards must be taken to protect the personal data when transferred.

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, if they are capable of industrial application, and lawful (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.

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). A work is

eligible for copyright protection provided that it represents 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 rules or laws that apply to academic technology transfers in your jurisdiction?

Higher education is a competition of the Communities in Belgium. For the Flemish Community, the Codex Higher Education stipulates that any property rights to inventions made by salaried staff as part of their research duties shall belong exclusively to the university or the university college. The Codex further lays down rules for the participation of universities or university colleges in spinoff companies and for scientific services performed by universities and university colleges. Most academic technology or knowledge transfers are handled by the tech transfer offices of the universities or university colleges and take the form of license or other types of collaboration agreements or participation in spin offs.

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).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

The EPO has confirmed on multiple occasions and most recently in December 2021 that artificial intelligence (devices) cannot be named as inventors on patent applications.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The core rules and laws applicable to government funded inventions in Belgium are noted down in the Belgian Code of Economic Law, Book XI, Title 1, Chapter 2. Irrespective of any governmental funding, the inventor is considered the person who developed the invention.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The allocation of intellectual property rights must be carefully assessed before concluding collaborative agreements. Both the ownership of results and the IP that arises from such results as potential licence rights and the limits to such licence rights must be considered before R&D commences.

7.2 What considerations apply in agreements between healthcare and non-healthcare 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 which can lead to more holistic care strategies that could improve patient outcomes. In this context, ML can help healthcare organisations meet growing medical demands, improve operations and lower costs, which is especially valuable for a sector characterised by limited resources. Besides, ML can help practitioners detect and treat diseases efficiently and with more precision and more personalised 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 only 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 regard to patents, according to the European Patent Office and Article XIV §1, 4 of the CEL, 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 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 the AI (the researcher).

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

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 solutions?

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 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?

Caution should be exercised when making use of cloud-based services, as this is an area particularly sensitive to data breaches, cybersecurity issues and other data protection hazards. If a (digital) health company/healthcare organisation makes use of the services of a cloud service provider, such service provider will generally be considered the processor, which processes personal data on behalf of the company or organisation (controller) and which may be working with multiple subprocessors. Consequently, a sound data processing agreement must be concluded, including extensive audit rights for the controller and a liability clause that sufficiently protects the controller in the event of claims by data subjects or a data protection authority as a result of infringements by the processor. Furthermore, the healthcare industry is notably vulnerable to cyber-attacks, therefore it is of utmost importance to ensure that cloud service providers offering services to the (digital) health industry have taken adequate organisational and technical measures to safeguard any personal data and confidential documents stored. In this regard, the Act establishing a framework for the security of network and information systems of general interest for public security (transposition of European Directive (EU) 2016/1148 of 6 July 2016) must be kept in mind, which aims to ensure a high level of security for essential service providers such as hospitals and which is currently under revision at the European level (NIS 2 Directive).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare 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 NIHDI.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare 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. 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.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The lack of reimbursement for a great number of digital health solutions is one of the major deficiencies in the Belgian (regulatory) landscape. In addition, uncertainty regarding the interpretation of existing legal frameworks on new health technology hinders swift adoption. Although the primary responsibility for healthcare remains with the Member States, a more harmonised approach on EU level may benefit the cross-border offering of digital healthcare services and products. Finally, it needs to be noted that although the government already initiated certain financial incentives for health practitioners to implement electronic health records, such incentives may need to be extended to other digital health applications.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The NIHDI is responsible for the accreditation of physicians and pharmacists, while organisations such as the Joint Commission International accredits hospitals in Belgium. As the NIHDI is also the institution responsible for reimbursement decisions (see question 10.6), naturally, its endorsement of digital health solutions is essential to steer clinical adoption. In addition to the NIHDI, the guidance and advice of the deontological body of physicians – the NCOP – are crucial in the long road ahead to better patient care through digital health.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Digital health solutions that are medical devices can be reimbursed by the NIHDI if they fulfil the reimbursement criteria (see question 3.1 above). However, other digital health solutions and telehealth services are currently not part of the nomenclature of the NIHDI and therefore not currently reimbursed.

Olivier Van Obberghen 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.

Quinz
Medialaan 28B
1800 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.

Quinz
Medialaan 28B
1800 Vilvoorde
Belgium

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

Amber Cockx is a Life Sciences lawyer with a main focus on technology and data protection matters. 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
1800 Vilvoorde
Belgium

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

Wietse Vanpoucke is a lawyer focusing on the life sciences industry, including digital health. Within this industry, clients ranging from innovative start-ups ventures to multinational corporations call on Wietse's counsel to support and advise in (strategic) transactions and European regulatory affairs, throughout the entire product life cycle. In this context, his main areas of expertise comprise of negotiating and drafting agreements, all aspects of data protection and privacy laws, medical devices, software applications and emerging technologies such as artificial intelligence and blockchain.

Quinz
Medialaan 28B
1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: wietse.vanpoucke@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). Its Life Sciences department is headed by Pieter Wyckmans and Olivier Van Obberghen.

www.quinz.be

Brazil


Ana Karina E. de Souza


Elton Minasse


Juliana Abrusio

Machado Meyer Advogados

1 Digital Health

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. It also includes 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 digital health technologies in your jurisdiction?

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, contributing to the improvement of clinical and hospital processes and assisting in managing information at these locations. An example of artificial intelligence in use 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 technology to remotely perform diagnostics and monitor patients.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues for digital health in Brazil are: (i) the difficulty in ensuring 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.

1.4 What is the digital health market size for your jurisdiction?

Digital Health comprises the use of Information and Communications Technology (**ICT**) resources for producing and providing reliable information about the health status of those who need it when it is needed. According to Brazil's 2019–2023 National Digital Health Strategy Action, Monitoring and Evaluation Plan issued by the Federal Government, the National Digital Health Strategy Action, Monitoring and Evaluation Plan first step objective is the implementation of a National Health Data Network (**RNDS**). This is a nationwide health data integration platform intended to drive the information exchange among the Healthcare Network (**RAS**), enabling the care transition and continuity in both public and private sectors. Based on the integration of both initiatives, the 'Conecte SUS' programme has arisen, characterising the essence of the first step of the 2019–2023 period.

Besides the federal actions, the private market is also growing. According to the Market Data Forecast analysis, in Latin America, 47% of the market share is accounted by Brazil's digital healthcare market.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

Please note this information is subject to market analysis provided by relevant companies in this regard. The five largest Brazilian healthtech start-ups, highlighted by the consulting firm Distrito, by criteria such as revenue, headcount, visibility

(followers on social networks) and funding, for instance, are: Dr Consulta; Pixeon; Vitta; iClinic; and Memed. Please also consider that traditional healthcare companies have started developing digital solutions in order to provide their services via the Internet, but their financial data is not always disclosed.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The Brazilian healthcare system was constitutionally determined to be universal, decentralised, full-service, and of communal participation. It is therefore the case that Brazil provides its people with ubiquitous healthcare free of charge. Nevertheless, the legal framework on digital health is still in its inaugural phase, in which its premises and foundations are being determined.

Consolidation Ordinance No. 1, issued on September 28, 2017, established the Digital Health Strategy to be carried out between 2020 and 2028 in Brazil (**ESD28**), instituting the general guidelines for governmental measures to be taken regarding digital health until 2028. The ESD28 is composed of two instruments: the Action Plan for Digital Health 2020–2028; and the Monitoring and Evaluation (**M&E**) Plan for Digital Health.

The same Ordinance determined that the Action Plan for Digital Health shall contain: (i) the set of actions and sub-actions to be executed; (ii) the resources of the area for the implementation of the ESD28; and (iii) the appointing of a person responsible for carrying out the actions and sub-actions and for their periodic monitoring.

On the other hand, the Digital Health Monitoring and Evaluation Plan must contain: (i) the necessary activities to achieve the actions and sub-actions provided for in the Action Plan, ensuring that it remains consistently and systematically adhered to the ESD28 vision; and (ii) health indicators, targets, mechanisms, and methodologies to assess the implementation of the ESD28.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The Brazilian Federal Constitution establishes in article 196 that health is a right of the people and a duty of the State, and shall thus 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 No. 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 No. 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 be analysed by the Federal Council of Medicine regarding several aspects such as safety, efficiency, convenience and benefits to patients.

Law No. 13,989, of 15 April 2020, which authorises the use of telemedicine during the crisis period caused by the COVID-19 pandemic.

In addition, Brazilian 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 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 Civil Framework of the Internet (Law No. 12,965/2014) and its regulating decree (Decree No. 8,771/2016) set forth the guidelines for Internet use in the country, 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 data 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 Unico de Saúde*, **SUS**).

The Electronic Health Record Law (Law No. 13,787/2018) provides for the digitalisation and use of computerised systems for the 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 being 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 this programme, the Ministry has assigned 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.

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

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

"Mhealth" is the medical and public health practice performed through mobile devices such as smartphones, patient monitoring devices, personal digital assistants, and other wireless gadgets. 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 healthcare devices and software 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 charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

Regarding regulatory authorities, the following stand out: (i) the Ministry of Health; (ii) ANS; (iii) ANVISA; and (iv) CFM.

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 for the population.

ANS is the regulatory agency linked to the Ministry of Health, and is responsible for the health insurance sector in Brazil. Its task is to promote the defense of public interest in supplementary healthcare, regulate sector operators – including their relations with service providers and consumers – and contribute to the development of health actions in the country.

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, CFM aims to oversee professional ethics throughout the country and, at the same time, judge and regulate the medical profession through regulatory action.

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

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.

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 regulations (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.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

There is no comprehensive regulation in Brazil with respect to the application of artificial intelligence in medical procedures, although it is already a reality and in practice. The absence of proper regulation gives cause to legal uncertainty, especially on cases related to product liability and/or professional malpractice. Please note that the legal framework indicated in question 2.2 above is applicable.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**

  Resolution No. 1,643/2002 of CFM defines telemedicine as "*the practice of medicine through the use of interactive methodologies of audiovisual communication and data, with the objective of health assistance, education, and research*". It is the administrative act that defines and establishes rules for telemedicine. In accordance with the resolution, the physician who issues the report at a distance can only provide diagnostic and therapeutic support in case of an emergency, or when the responsible doctor requests, in this regard.

  In the context of the COVID-19 pandemic crisis, Brazil issued legislation about telemedicine. Based on that, CFM in March 2020 issued to the Ministry of Health the CFM Office No. 1756/2020-Cojur, which recognised the possibility of the use of telemedicine, especially in the context of the COVID-19 pandemic.

  Following that, in April 2020, Brazil approved the Telemedicine Law No. 13,989/2020 authorising the use of telemedicine during the crisis caused by the COVID-19 pandemic. It determines in its article 3 that telemedicine means, *inter alia*, the practice of medicine mediated by

technologies in order to assist, research, prevent diseases and injuries, and promote health. CFM pronounced in the same month clarifications and measures by virtue of Law No. 13,989/2020.

Despite the difficulties faced, Brazil has clearly demonstrated advances on the regulation of telemedicine. However, there had not been any official manifestation regarding the authorised use of telemedicine after the pandemic. It is definitely a matter to be considered in the face of the different possibilities COVID-19 has showed to the population.

It should be noted that in Federal Law No. 13,709/2018, 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. The LGPD has limited the legal basis by which such personal data can be processed, as well as having increased the level of responsibility of data controllers. When adopting telemedicine, people should be aware of the rules and principles of personal data in Brazil set forth in the LGPD, notably those related to sensitive data.

- **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 in practice. The absence of proper regulation gives cause to legal uncertainty, especially on cases related to product liability and/or professional malpractice.

General provisions of the Consumer Defence Code apply with respect to product liabilities regarding: wearables, virtual assistants; mobile apps; Software as a Medical Device; clinical decision support software; AI/ML powered digital health solutions; Internet of Things (**IoT**) and connected devices; 3D printing/bioprinting; digital therapeutics; and natural language processing. There is no specific regulation at the moment related to any of these categories. 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.

Product and service liability: the Consumer Defence Code sets forth strict liability in connection to the malfunctioning and defects of products and services. It also establishes an obligation for providers to be accurate and transparent when providing 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 about health conditions. Furthermore, in the absence of provisions regulating liabilities arising out from the use of new technologies, such as AI and ML, providers will assume all risks connected to the use of such technology in association with "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 to observe 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 the LGPD, especially for sensitive personal data. Specific or separate 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 million. 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 the health information of a data subject in order to obtain an 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, are already comprehensive in terms of the rights that individuals are entitled to when contracting with digital platforms. It is expected that new technologies (AI, ML, 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 shall 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 entered into force in September 2021, 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 million 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 bases. Particularly, sensitive personal data processing may be subject to specific and separate 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 with 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 the 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.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Data is intrinsically connected with essential rights of freedom and personal relevant information. The LGPD, which is the statute that rules personal data processing activities in Brazil, is changing the way in which the protection of personal data is ruled and handled, creating a microsystem of rules that impacts all sectors of the economy.

The LGPD establishes a new legal framework to be observed in the processing of personal data, providing the rights of personal data subjects, the legal bases that allow the processing of personal data, obligations and requirements related to information security incidents, data breaches and transferences of personal data, including cross-border transactions, as well as the sanctions to be applied in case of non-compliance.

In addition, the LGPD created the ANPD, responsible for preparing guidelines and applying administrative sanctions in case of non-compliance with the LGPD.

When discussing health, it is important to highlight that health information that is related to an individual is considered to be sensitive personal data under the LGPD. With respect to health information, the LGPD set forth that, as a rule, such information shall not be processed to obtain economic advantages. Liability connected to violation of the LGPD with respect to sensitive personal data is also addressed in the law.

Moreover, considering the importance of the correct collection and use of personal data, processing agents should observe the law otherwise penalties shall be applicable. In the current scenario (prior to the effectiveness of the administrative sanctions provided for in the LGPD), failure to comply with any provisions of such legislation has as its risks: (i) the filing of lawsuits, individual or collective, claiming damages resulting from violations, based not only on LGPD, but also on the sparse sector legislation on data protection still in force; and (ii) the application of penalties provided for in the Consumer Defense Code and Internet Civil Framework, when the activity is performed through the Internet, by consumer protection agencies, since these have already acted in this sense, even before the LGPD and the effective structuring of ANPD, especially in cases of security incidents resulting in improper access to personal data. In addition, in August 2021, the LGPD sanctions will come into effect, including, but not limited to, warnings,

mandatory public disclosure of our non-compliance, temporary blocking and/or deletion of the personal data pertaining to the offence, a fine of up to 2% of our post-tax revenue (or that of our group or conglomerate in Brazil) for the most recently completed fiscal year, as well as daily penalties, up to a total amount of R$50 million, and partial or total prohibition of performing the activities relating to the data processing, among others.

Lastly, secure comprehensive rights to data that are used and/or collected is essential in Brazil. The priority is to protect personal data every possible way, not only because it is the law, but also in the view of the related penalties.

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 specific data subjects 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 to 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:

- **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.
  - **Utility model patent**: any object of practical use, or part thereof, that is susceptible to industrial application, presents a new shape or arrangement and involves an inventive act that causes a functional improvement in its use or manufacture.
- **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 National Institute of Industrial Property (**INPI**), 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 a 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; or
  - 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 to 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 proof of payment 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 a 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
  - 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 for copyright registration to enforce such rights against third parties. All 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 their 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 be fixed in any form;
  - musical compositions, with or without words;
  - audio-visual works, with or without sound;
  - photographic works and related works;
  - drawings, paintings, sculptures, geographical maps, plans, sketches and related works;
  - 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: the 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 1st 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 license**: must 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 analogue 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 1st January of the year following its registered publication or, when such register is unavailable, its creation. Similarly to 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; or (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.

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 someone 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 the industrial property rights violation and unfair competition that are not provided in the Industrial Property Law, but tend to prejudice another's violation had not occurred, and the benefits gained by 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; or
  - loss of profits will be determined by the following criteria which is the most favourable to the injured party: (i) the benefits that the injured party would have gained if the author of the rights' violation; or (ii) the remuneration that the author of the violation has paid to the owner of the violated rights for a granted licence which would have legally permitted him to exploit the rights.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

In Brazil, the main rules related to academic technology transfers are provided in the Federal Law No. 10,973/2004 (Innovation Law), as amended by the Federal Law No. 13,243/2016, and detailed by the Federal Decree No. 9,283/2018.

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 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 a patent. The software itself would not in principle be subject to patent protection.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

Brazilian legislation does not expressly provide the need for the inventor of a patent to be a human being.

However, there are many parts of the legislation that indirectly indicates the need for inventors to be human beings, for example, paragraph 3 of article 6 of Federal Law No. 9,279/96 (Industrial Property Law), which allows inventors to disclose their name, the sole paragraph of article 12 of such law, which requires an inventor's declaration regarding disclosure, and more specifically, article 5 of the Brazilian Federal Constitution, which grants individuals temporary privilege over industrial inventions.

Therefore, the National Institute of Industrial Property (**INPI**) strictly follows Brazilian legislation and grants patent registration only to individuals or legal entities.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The following rules are applicable to government-funded inventions:

- Federal Law No. 10,973/2004 (Innovation Law), as amended by the Federal Law No. 13,243/2016, and detailed by the Federal Decree No. 9,283/2018; and
- Federal Law No. 9,279/96, the Industrial Property Law.

Additionally, in Brazil, there are several government institutions/agencies that promote research and technology and each one is governed by its specific law; they are: CNPQ (Federal Law No. 6129, of 6 November 1974); CAPES (Federal Law No. 8405, of 9 January 1992); INEP (Federal Law No. 9,448, of 14 March 1997); FAPESC (State Law No. 14,328, of 15 January 2008); FAPESP (State Law No. 5.918, of 18 October 1960); the Ministry of Science and Technology; and the Ministry of Health.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Controller and processor considerations apply to collaborative improvements.

7.2 What considerations apply in agreements between healthcare and non-healthcare 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?

As of today, there is no regulation yet in Brazil regarding ML 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 applies 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 ML 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 ML 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 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 the protection of databases. However, in order for such database to be protected, it must be organised in a creative and unique manner, so it constitutes an intellectual creation. Although it is unlikely that the databases used in ML 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 solutions?

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 the general and the Civil Framework of the Internet. The Consumer Defence Code sets forth strict liability in connection to malfunctioning and defects of products and services. It also establishes the obligation for 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 ML, providers will assume all risks connected to the use of such technology in association to products and services commercial claims.

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 for 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 permitted 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 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 abovementioned 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.

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 Services), 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-healthcare companies should consider before entering today's digital healthcare 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 healthcare 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.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

From a legal point of view, the uncertainty on the matter is a key barrier. It is possible to mention the lack of a specific regulatory framework to organise the topic, since several statutes and administrative acts were issued without any arrangement among them; and also, the existence of several authorities regulating the sector, including the possibility of regulation through the judiciary.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Under Brazilian jurisdiction, the official requirement for digital health solutions is the approval of the competent public authority, as opposed to clinician certification bodies, which could include, for instance, the Ministry of Health, ANVISA, and/or CFM. The approval may vary based on the type of technology to be considered but shall always depend on the competent public authority's endorsement.

On the other hand, ANVISA's Resolutions No. 185/2001 and No. 40/2015 regulate the licensing requirements applicable for medical devices for health and diagnostics. Among the types of medical devices that may be subject to be approved by ANVISA are software that act as health products.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

As previously mentioned, the Brazilian government provides its population with a universal healthcare system free of charge. Although digital health is currently a work in progress, there are several governmental digital instruments within the healthcare scope made available to the people. *Conecte SUS*, for instance, is an application software that consolidates one's medical information and allows for the scheduling of medical appointments at no cost.

Private insurers, on the other hand, have achieved providing real-time teleconsultations on medical matters through application software. Such teleconsultations have been allowed since Resolution CFM No. 1,643 was issued on 7 August 2002, however, limited to emergency situations. Ultimately, on 15 April 2020, Law No. 3,989 was issued, recognising the use of telemedicine for consultations, pre-clinical care, care support, diagnosis and monitoring. Although the law allows for a broader use of telemedicine only while the COVID-19 crisis lasts, it is expected that further legislation on the matter shall come to be in the near future, regulating telemedicine under circumstances unrelated to the COVID-19 pandemic.

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 Ana'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. Ana has previous experience in the provision of legal assistance to clients of several areas of knowledge, such as energy, oil and natural gas, mining, transport, sanitation and pharmaceuticals.

Machado Meyer Advogados
Av. Brigadeiro Faria Lima, 3200 – Jardim Paulistano
São Paulo – SP, 01451-000
Brazil

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

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. Elton has previous experience in areas of knowledge such as automotive, banking, electronic commerce, electronics, logistics, and retail.

Machado Meyer Advogados
Av. Brigadeiro Faria Lima, 3200 – Jardim Paulistano
São Paulo – SP, 01451-000
Brazil

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

Juliana Abrusio works in the areas of digital law and personal data protection, including information security (DLP, regulations, policies, incidents and training), response to data leakage, due diligence, electronic contracts, digital fraud, among other topics. She also provides services related to administrative litigation before the ANPD and judicial litigation involving digital law and data protection. Juliana experience in the legal structuring of new digital business models (fintech, agrotech, edutech, heathtech, insurtech), as well as in markets involving blockchain and cryptocurrencies. In addition, she advises companies that use artificial intelligence (big data and data analytics). Additionally, Juliana works in consulting in the areas of gaming and e-Sports, innovation and start-ups.

Machado Meyer Advogados
Av. Brigadeiro Faria Lima, 3200 – Jardim Paulistano
São Paulo – SP, 01451-000
Brazil

Tel: +55 11 3150 3311
Email: jabrusio@machadomeyer.com.br
URL: www.machadomeyer.com.br

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, the 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

China


Cindy Hu


Jason Gong


Jiaxin Yang

East & Concord Partners

1 Digital Health

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

Digital health is not a legal term defined under the laws and regulations of the People's Republic of China ("PRC") but is frequently referred to in commercial contexts and industry policies.

Digital health usually refers to the development and use of digital technologies to popularise health knowledge and its implementation to related fields, covering the application of digital technologies such as the Internet of Things ("IoT"), artificial intelligence ("AI"), and big data in medical services and health management. Digital health usually utilises technologies such as big data and AI to provide solutions for medical treatment, clinical research, drug development, imaging diagnosis, health management and other medical and healthcare needs.

1.2 What are the key emerging digital health technologies in your jurisdiction?

The key emerging digital health technologies include AI, mHealth, wearable devices, robotics, 3D printing, blockchain, global positioning system ("GPS") technology and 5G technology.

1.3 What are the core legal issues in digital health for your jurisdiction?

Personal privacy protection and data security are the core legal issues in digital health. In addition, the monopoly of healthcare data, the liability for medical damage caused by medical AI, and the ethical risks brought by the application of AI diagnosis and treatment technology are also common legal issues in digital health.

1.4 What is the digital health market size for your jurisdiction?

Influenced by COVID-19, China's online medical advantages have been highlighted, and the market share of digital health has increased continuously. According to the digital health report "Analysis Report of China's Digital Health Industry in 2021 – Research on the Current Situation and Future Prospect of Industrial Scale", the number of online medical users had reached 215 million by December 2020, accounting for 21.7% of the total number of Internet users. The revenue of China's digital health market was CNY 218.1 billion in 2019, and is expected to increase to CNY 4,222.8 billion in 2030, with a compound annual growth rate of 30.9%.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

According to the List of Chinese Digital Health Enterprises released by the 2021 China International Digital Economy Exposition, the five largest digital health companies in China are Ping An HealthKonnect (intelligent medical insurance integration platform), JD Health (online pharmacy), We Doctor (Internet hospital), United Imaging (innovative medical devices) and MGI Tech (innovative medical devices).

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The core healthcare regulatory schemes related to digital health include the following:

- Law of the PRC on the Promotion of Basic Medical and Health Care.
- Regulation on the Administration of Medical Institutions.
- Administrative Regulations on Application of Electronic Medical Records (for Trial Implementation).
- Administrative Measures on Standards, Security and Services of National Healthcare Big Data (for Trial Implementation).
- Administrative Measures for Internet-based Diagnosis (for Trial Implementation).
- Administrative Measures for Internet Hospitals (for Trial Implementation).
- Administrative Regulations on Telemedicine Services (for Trial Implementation) ("Administrative Regulations on Telemedicine Services").

- Guiding Opinions of the State Council on Vigorously Advancing the "Internet Plus" Action.
- Opinions of the General Office of the State Council on Promoting the Development of "Internet Plus Health Care".
- Notice of the National Health Commission's office on the Pilot Work of "Internet Plus Nursing Service".
- Guiding Opinions of the National Healthcare Security Administration on Improving the "Internet Plus" Medical Service Price and Medical Insurance Payment Policy.
- Guiding Opinions of the National Healthcare Security Administration on Actively Promoting the Medical Insurance Payment Work of "Internet Plus" Medical Services (Guiding Opinions of "Internet Plus" Medical Services).
- Information Security Technology-Guide for Health Data Security (GB/T 39725-2020).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The other core regulatory schemes include the following:

- Civil Code of the PRC ("Civil Code").
- Anti-Unfair Competition Law of the PRC ("Anti-Unfair Competition Law").
- Cybersecurity Law of the PRC ("Cybersecurity Law").
- Data Security Law of the PRC ("Data Security Law").
- Personal Information Protection Law of the PRC ("Personal Information Protection Law").
- Measures for Cybersecurity Review.
- Interim Provisions on Banning Commercial Bribery.
- Administrative Regulations on Human Genetic Resources of the PRC.
- Measures for the Administration of Population Health Information (for Trial Implementation).
- Measures for the Management of Scientific Data.
- Information Security Technology – Personal Information Security Specification (GB/T 35273-2020).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The regulatory schemes which apply to consumer healthcare devices or software in particular, include the following:

- Law of the PRC on the Protection of Consumer Rights and Interests.
- Product Quality Law of the PRC ("Product Quality Law").
- E-Commerce Law of the PRC.
- Regulations on the Supervision and Administration of Medical Devices ("Medical Devices Regulations").
- Rules for the Classification of Medical Devices.
- Administrative Measures on the Registration and Recordation of Medical Devices.
- Measures for the Supervision and Administration of Medical Device Production.
- Measures for the Supervision and Administration of Business Operations of Medical Devices.
- Measures for the Supervision and Administration of Online Sale of Medical Devices.
- Guiding Principles for Technical Review of Medical Device Software Registration.
- Guiding Principles for Technical Review of Network Security Registration of Medical Devices.
- Guiding Principles for Technical Review of Mobile Medical Device Registration.
- Guiding Principles for Classification and Definition of Artificial Intelligence Medical Software Products ("Guiding Principles for AI Medical Software Products").
- Classification Catalogue of Medical Devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The principal regulatory authorities include the following:

- The National Health Commission ("NHC"): The NHC primarily formulates and enforces national health policies and regulations pertaining to healthcare services, healthcare institutions and healthcare professionals. Internet-based diagnosis and treatment and remote consultations between healthcare institutions are both regulated by the NHC.
- The National Medical Products Administration ("NMPA"): The NMPA regulates drugs, medical devices and cosmetics, and is responsible for the safety, supervision and management of standard formulation, registration, manufacturing and post-market risk management.
- National Healthcare Security Administration ("NHSA"): The NHSA is primarily responsible for formulating and implementing policies related to basic medical insurance ("BMI"), such as reimbursement, pricing and the procurement of drugs, medical consumables and healthcare services.
- Ministry of Industry and Information Technology ("MIIT"): The MIIT is responsible for the management of the Internet industry, the access management of the information and communication industry, and the construction of network and information security guarantee system in the information and communication field. In terms of digital health, MIIT is responsible for supervising relevant technology development, personal data protection, etc.
- Cyberspace Administration of China ("CAC"): The CAC is responsible for the overall planning and co-ordination of network security and relevant supervision and administration, including regulating the cross-border transfer of healthcare data, cybersecurity review of Internet hospitals, network personal privacy and information protection.
- State Administration for Market Regulation ("SAMR"): The SAMR is responsible for supervising the market order in market transactions, online commodity transactions and related services, and organising the investigation and punishment of illegal medical advertisements, Anti-Commercial-Bribery and other acts against unfair competition.
- The Ministry of Public Security ("MPS"): The MPS is responsible for enforcing the Cybersecurity Classified Protection System and investigating cybercrimes, including conducting inspections and recording filings for the related system completed by healthcare institutions (Internet hospitals are included), and investigating crimes related to infringement of personal data and illegal access to information systems.

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

Personal information protection, data security and cybersecurity are the key areas of enforcement in relation to digital health.

China has established the Personal Information Protection Law (effective since November 1, 2021), the Data Security Law and the Cybersecurity Law. The Multi-Level Protection Scheme ("MLPs") implemented in the field of cybersecurity, as a compulsory legal obligation stipulated by the Cybersecurity Law and relevant regulations, has become a main focus in enforcement in most industries, including digital health.

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

The main applicable laws and regulations include: Medical Devices Regulations; Rules for the Classification of Medical Devices; Administrative Measures on the Registration and Recordation of Medical Devices; Measures for the Administration of the Clinical Use of Medical Devices; and Guiding Principles for AI Medical Software Products.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

In addition to the relevant regulatory provisions applicable to medical devices, AI/Machine Learning ("ML") powered digital health devices or software solutions shall also comply with the Management Specification of AI Aided Diagnosis Technology and Management Specification of AI Aided Therapy Technology in terms of Special requirements for medical institutions to carry out AI-aided diagnosis technology and AI-aided treatment technology in relation to department setting, staffing, technical management, etc.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Medical institutions shall comply with the Administrative Regulations on Telemedicine Services in terms of personnel setting, equipment and facilities, telemedicine service process, responsibility sharing and management.
- **Robotics**
  The liability arising out of medical accidents caused by robots is difficult to identify, and the division of responsibilities among producers, operators and users of intelligent robots is more complex.
- **Wearables**
  In accordance with Medical Devices Regulations and Rules for the Classification of Medical Devices, some wearables (such as hearing aids or pain relief therapeutic instruments) are regarded as medical devices, and are subject to the relevant regulatory requirements on medical devices.
- **Virtual Assistants (e.g. Alexa)**
  For virtual assistants like Siri and Alexa, problems such as eavesdropping, leakage of personal privacy and information may occur.
- **Mobile Apps**
  Mobile medical APPs involves patients' electronic medical records, health records, consultation information and image data, and is highly dependent on the network and information technology. When cybersecurity or technical security is attacked or threatened, privacy and information leakage may occur.
- **Software as a Medical Device**
  In accordance with Medical Devices Regulations, Rules for the Classification of Medical Devices, and Guiding Principles for AI Medical Software Products, Software as a Medical Device ("SaMD") will be subject to the relevant regulatory requirements on medical devices.
- **Clinical Decision Support Software**
  In accordance with Medical Devices Regulations, Rules for the Classification of Medical Devices, and Guiding Principles for AI Medical Software Products, it may be subject to the relevant regulatory requirements on medical devices.
- **AI/ML powered digital health solutions**
  Please refer to question 2.7.
- **IoT and Connected Devices**
  Most of the data stored or collected by the Internet of Things ("IoT") terminal belongs to sensitive medical information. Once important information is leaked or maliciously modified by hackers, it will lead to cybersecurity, data and information leakage problems.
- **3D Printing/Bioprinting**
  The application of 3D bioprinting in medical treatment is still in the early stage of exploration, and no specific provisions for 3D bioprinting have been issued in China.
- **Digital Therapeutics**
  At present, digital therapy products are generally supervised as a medical device, and are subject to relevant regulatory requirements on medical devices.
- **Natural Language Processing**
  Natural language processing involves a large number of personal oral languages which are fed back to the natural language processing system for identification and processing and, therefore may lead to the problem of leakage of personal information and data.

3.2 What are the key issues for digital platform providers?

In terms of the healthcare sector, digital platform providers are highly regulated. In terms of industry access, digital platform providers need to apply for different business licences according to their business types, for example, where the business involves online data processing, voice and image communication and other business forms, the digital platform providers are required to obtain value-added telecom service qualification; where the digital platform providers provide users with drug and medical device information through the Internet, they shall obtain the qualification of an Internet drug information service. In addition, in the process of business operations, it is also necessary to comply with the above regulatory requirements on personal information protection, data security and cybersecurity.

4 Data Use

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

Some of the key issues for the use of personal data include how to standardise the code of conduct in such different links as collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information so as to ensure the rational use of personal information without infringement.

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

In addition to meeting the general provisions on the use of personal data, entities of different natures shall also comply with other relevant provisions, e.g.:

- If the entity involved is a third party that obtains relevant personal information through sharing or joint processing in accordance with the terms of the relevant agreement, it shall process the personal information in accordance with the relevant agreement, and shall not process personal information beyond the agreed processing purpose and method. If it infringes on individuals' rights and interests in terms of personal information and causes damage, it shall bear joint and several liability in accordance with the law.
- If the entity involved is located overseas and has one of the following circumstances: 1) providing products or services to domestic natural persons; 2) analysing and evaluating the behaviour of domestic natural persons; and 3) under other circumstances stipulated by laws and administrative regulations, the said entity shall establish a special institution or designated representative within the territory of the PRC to handle matters related to personal information protection, and submit the name of the relevant institution or the name and contact information of the representative to the relevant department responsible for personal information protection.
- If the entity involved falls within the definition of the critical information infrastructure operator ("CIIO"), it shall also abide by the Regulations on Security Protection of Critical Information Infrastructure.

4.3 Which key regulatory requirements apply?

The Personal Information Protection Law and other relevant laws and regulations stipulate the general rules on the collection and use of personal information. The use of personal information shall follow the principles of legality, legitimacy, necessity and integrity, and shall be open and transparent, and ensure the security and accuracy of personal information.

For example: 1) the data collection channel shall be legal, and advanced personal consent shall be obtained in accordance with the law. There must be an acknowledgment of the processing purpose, processing method, type of personal information processed, storage period, etc; 2) the processing of personal information shall have legal basis and shall not excessively collect personal information; and 3) personal information collectors shall formulate corresponding internal systems for information protection.

In addition, it should be noted that: 1) certain activities performed outside the PRC related to processing personal information of natural persons residing in the PRC will also be regulated by Chinese laws; and 2) when providing the personal information of those located outside of the PRC, one shall also comply with the following requirements: a) passing the security assessment organised by the national network information department; b) personal information protection certification by professional institutions; c) signing a contract with the overseas recipient according to the standard contract formulated by the national network information department to specify the rights and obligations of both parties; and d) special regulatory requirements of laws, administrative regulations or other conditions stipulated by the national network information department.

4.4 Do the regulations define the scope of data use?

According to the Personal Information Protection Law and other relevant provisions, the purpose, method and scope of processing personal information shall be clearly stated, and the processing shall be limited to the minimum scope to achieve the purpose of processing, and personal information shall not be excessively collected. The third party shall process personal information within the scope agreed by the individual on processing purpose, processing method and type of personal information.

In addition, the Information Security Technology – Personal Information Security Specification (GB/T35273-2020) provides detailed guidance on data use scenarios, assumptions and scope under various circumstances.

4.5 What are the key contractual considerations?

Where a contract is signed directly between an information processor with an information provider, the terms of the contract such as scope of data information processing, processing rules, exit restrictions, security measures, requirements for deletion, destruction or return of data and liability for breach of contract should be agreed on. The name and contact information of the personal information processor shall be informed in detail, and the purpose and method of processing the personal information, the type and retention period of the personal information processed, as well as other matters that are required to be informed according to laws and administrative regulations, shall be informed.

Where two or more personal information processors jointly process personal information, in addition to clearly specifying the above information, they shall also agree on their respective rights and obligations in the terms of the contracts.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The Civil Code clearly stipulates that a natural person's personal information shall be protected by law. For any unreasonable usage of personal information which infringes on the civil rights of individuals, the infringer shall bear civil liability according to law. For example, if a medical institution or its medical staff leak personal information, or disclose medical records without the consent of the patient, the medical institution shall bear tort liability.

The Criminal Law of the PRC stipulates corresponding criminal responsibility for infringement of citizens' personal information and violation of relevant laws.

In addition, those who violate relevant laws and regulations such as the Cybersecurity Law of the PRC, the Data Security Law of the PRC, the Personal Information Protection Law of the PRC or the Anti-unfair Competition Law of the PRC will also face corresponding civil, administrative and even criminal liabilities.

5 Data Sharing

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

The key issues to consider when sharing personal data include the following:

- whether the sharing of personal data complies with the principles of necessity and realisation of legitimate purposes;

- whether to inform and obtain personal consent;
- whether it meets the requirements of security measures necessary for data sharing;
- whether the contract signed by all parties to data sharing include terms such as: the processing purpose; duration; processing method; type of personal information; protective measures; and the rights and obligations of both parties;
- whether there is personal data that is prohibited from being shared; and
- whether a cross-border data transfer is involved.

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

In addition to meeting the general data sharing requirements, entities of different natures should also comply with other relevant provisions, for example: if the sharing party is the CIIO, it shall also abide by the Regulations on Security Protection of Critical Information Infrastructure.

However, if the receiving party is an overseas entity, specific conditions shall be met. For example, it has passed the security assessment organised by the national network information department, passed the personal information protection certification conducted by professional institutions, or entered into a contract with the overseas recipient according to the standard contract formulated by the national network information department to stipulate the rights and obligations of both parties.

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

Firstly, the provider of sharing data shall: 1) conduct the impact assessment of personal information protection in advance; 2) inform the individual of the recipient's name, contact information, processing purpose, processing method and type of personal information, and obtain the individual's consent; 3) agree with the recipient on the purpose of entrusted processing, time limit, processing method, type and protection measures of personal information, as well as the rights and obligations of both parties; and 4) supervise the recipient's processing activities of personal information.

Secondly, the recipient of sharing data shall: 1) process personal information according to the agreement, and shall not process personal information beyond the agreed processing purpose and processing method; 2) if the relevant contract is not effective, invalid, revoked or terminated, the personal information shall be returned or deleted and shall not be retained; 3) without the consent of the provider, the recipient shall not entrust others to process personal information; 4) the recipient shall also take necessary measures to ensure the security of personal information and assist the provider in performing its personal information protection obligations.

In addition, attention should also be paid to the regulatory requirements involved in the cross-border transfer of personal information. For example, the CIIO or the personal information processor who processes personal information up to the amount specified by the national network information department shall store within China the personal information collected and generated in China. If it is really necessary to provide it to an overseas recipient, the security assessment organised by the national network information department shall be passed. (If the laws, administrative regulations and national network information department stipulate that the security assessment may not be carried out, such stipulations shall prevail.)

In accordance with the Measures for Cybersecurity Review (issued on December 28, 2021, and effective on February 15, 2022), if network platform operators who hold personal information of more than 1 million users are to be listed abroad, they shall apply to the cybersecurity review office for cybersecurity review.

6 Intellectual Property

6.1 What is the scope of patent protection?

Any technical solutions by using natural laws can be the subject matter of invention patents or utility model patents. The design patent is one of the patent types stipulated in the Patent Law of the PRC, and it protects new designs of the whole or part of the product in terms of shape, pattern and/or colour. After a patent is granted, unless otherwise stipulated in the Patent Law of the PRC, no entity or individual may exploit the patent without the permission of the patentee.

6.2 What is the scope of copyright protection?

The subject matter of copyright protection covers various works, which refers to intellectual achievements that are original and can be expressed in a certain form in the fields of literature, art and science. Computer software is one of the forms of works stipulated in the Copyright Law of the PRC. According to the Copyright Law of the PRC, copyright includes both property rights and personal rights, of which property rights mainly include: reproduction rights; distribution rights; and rental rights.

6.3 What is the scope of trade secret protection?

In accordance with Chinese laws, a trade secret refers to commercial information such as technical information and business operation information not known to the public, which is of commercial value, and for which the rights holder has adopted corresponding confidentiality measures. In accordance with the Anti-unfair Competition Law, obtaining trade secrets by improper means, disclosing and using trade secrets obtained by others by improper means, disclosing and using trade secrets in his possession but in violation of confidentiality obligations, or abetting, luring and helping others to commit such acts are all acts of infringing trade secrets and corresponding civil liabilities can be imposed. Serious trade secret infringements are defined as a criminal offence under the PRC Criminal Law and is punishable by up to 10 years of imprisonment.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

In China, the laws currently applicable to the academic technology transfers include the Law on Scientific and Technological Progress of the PRC (revised in 2021), the Law on Promoting Transfer and Commercialization of Scientific and Technological Achievements of the PRC (revised in 2015) and Several Provisions on the Implementation of the Law on Promoting Transfer and Commercialization of Scientific and Technological Achievements of the PRC issued by the State Council of the PRC in 2016. Such laws and regulations have adjusted previous policies in this field and clarified that the project undertakers, on the premise of no conflict with national security or national/public interests, are legitimately authorised to own relevant intellectual property rights arising from the government funded projects. Furthermore, the

project undertakers are encouraged to legally transfer and commercialise these IP rights in various ways. However, any transfer or exclusive license to an overseas company shall be approved by the project administration organisation.

Public universities are conducting pilot programmes in guiding scientific researchers to transfer and commercialise IP rights in line with the laws. According to a document jointly issued by four national-level Ministries in 2020, Chinese universities will gradually establish disclosure systems for service inventions, establish and perfect technology transfer and IP management and operation departments, and explore the reforming of ownership of service inventions, such as division of ownership between universities and researchers, as well as permitting the scientific researchers to apply for patents in the form of non-service inventions in the event the university declines to apply for service patents.

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

SaMD enjoys two forms of protection in China. Firstly, as it is regarded as a type of work protected under copyright, it does not require an application and examination process. Although the protection period is long, the disadvantage is that it is a form of expression which is capable of copyright protection and not a technical idea. Secondly, SaMD can be protected as it is considered an invention patent. It should be noted that pure algorithms or calculation rules are unpatentable subject matter under the Patent Law of the PRC: only when the technical features of the hardware are included in the claims can it be considered to be protected. Unlike copyright, what is protected by patent is the technical solution itself and, therefore this type of protection is thought to be more powerful.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

In accordance with the current laws and regulations of the PRC, an inventor refers to a person who has made creative contributions to the substantive characteristics of an invention. It is generally understood that the inventor should be a natural person and, therefore, based on the current effective laws and regulations AI devices are unlikely to be recognised as inventors in China.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

Please refer to question 6.4.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

In the case of collaborative improvements, a written contract is required to agree on the rights and obligations of each party, and it is necessary to take into account how to handle the failure of collaborative improvements, as well as the ownership and use of rights of patents and non-patented technologies generated in the collaboration. In the absence of such a written contract, according to the provisions of the Civil Code, the right to apply for a patent shall be jointly owned by the parties to the collaborative improvements. If one party transfers the patent application right jointly owned with other parties, the other parties shall have the priority to such transfer under the same conditions. If there is no agreement or the agreement is not clear about the non-patented technological achievements, all parties have the right to use and transfer such achievements.

For Sino-foreign collaborative improvements, it is also necessary to consider the possible application of some mandatory laws and regulations. For example, if Chinese human genetic resources are involved, especially in cases exporting Chinese human genetic resource materials, according to the provisions of the Biosecurity Law of the PRC, an approval from the competent department shall be obtained. Furthermore, as for the technological achievements produced by using Chinese human genetic resources to carry out international cooperative research, the patent rights shall be jointly shared by the parties according to the Administrative Regulations on Human Genetic Resources of the PRC.

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

When signing agreements with non-healthcare companies, in addition to meeting the above requirements for data sharing, transmission and other processing, healthcare companies shall ensure that non-healthcare companies comply with the national and industrial regulations and requirements of the business they are engaged in, have the necessary business qualifications, have the abilities to implement relevant laws and regulations, implement relevant standards and guarantee data security, and have a comprehensive management system.

According to the Measures for Cybersecurity Review, if a healthcare company qualifies as a CIIO, when it purchases network products and services, it shall anticipate the potential national security risks after the products and services are put into use. Those products and services that affect or may affect national security shall be reported to the cybersecurity review office.

8 AI and Machine Learning

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

As a common form of AI, machine learning is widely used in AI-aided diagnosis and treatment, medical imaging, wearable devices, genetic testing, pharmaceutical research, personal health management, and hospital management, etc.

8.2 How is training data licensed?

Data licensing in AI involves the licensing of relevant intellectual property rights, such as patents, software copyrights and trade secrets, and the licensed use shall apply to the Anti-Unfair Competition Law, the Patent Law of the PRC, the Regulations on the Protection of Computer Software and relevant provisions.

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 existing effective laws and regulations, AI can neither be an author in the context of the Copyright Law, nor an inventor or designer in the context of the Patent Law. As a result, the existing laws and regulations do not cover this area.

However, with the rapid development of AI technology, the legislation of intellectual property protection of AI-generated content is an important issue which needs to be urgently addressed. Chinese academia has been holding discussions on this issue as well. However, to date there is no unified understanding or relevant legislative proposals.

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

Licensing data for use in machine learning in a business context mainly includes the applicable scope of licensing (duration, territory, sub-license or not), restrictions of data use, non-competition and confidentiality.

9 Liability

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

The Civil Code, the Product Quality Law, Administrative Regulations on Telemedicine Services and relevant provisions have specified the liabilities of adverse outcomes in digital health solutions.

Where defects in medical devices and other digital health products cause personal injury or damage to others, victims may claim compensation from the manufacturer of the products or the vendor of the products. After one party makes compensation, that party has the right to seek indemnification from other parties who may be held liable.

If any damage or harm to a patient is caused during the course of diagnosis and treatment by the defects of digital health products, such patient may request compensations from the manufacturer or the relevant medical institution. After making the compensation, the relevant medical institution has the right to recover the losses from the liable medical device manufacturer.

When a dispute occurs in the course of remote medical services, the inviter shall bear corresponding legal liabilities for remote consultation, and the inviter and the invitee shall jointly bear corresponding legal liabilities for remote diagnosis. In terms of remote consultation, where medical institutions conduct remote consultation, the invitee shall provide diagnosis and treatment opinions, and the inviter shall specify the diagnosis and treatment plan. In terms of remote diagnosis, where an inviter and invitee establish a counterpart support or form a medical consortia and other cooperative relationships, the inviter shall carry out auxiliary examinations such as medical imaging, pathology, electrocardiograms, and ultrasound, the invited medical institution at a higher level shall conduct diagnosis, and the specific process shall be specified by the inviter and invitee through an agreement.

9.2 What cross-border considerations are there?

According to the relevant provisions of the Personal Information Protection Law, where a personal information processor needs to provide personal information to any party outside China, it should first obtain the individual's consent and conduct advanced assessment of the impact on personal information protection. If the data involves medical and health data, advanced security assessment and review shall also be carried out.

Pursuant to the Special Administrative Measures (Negative List) for Foreign Investment Access (2021 version), the provision of medical services by foreign medical service providers in China is limited to the form of Sino-foreign joint ventures, and foreign medical service providers shall not establish medical institutions in China in the form of sole proprietorship. In addition, foreign investment in the development and application of human stem cells, genetic diagnosis and treatment technologies is prohibited in China.

Where imported digital medical devices are involved, registration or filing of medical devices shall be completed according to the Medical Devices Regulations and relevant provisions, and overseas applicants shall submit the application materials to the medical products regulatory authority through a domestic enterprise, as well as the documents certifying the approval of the marketing of such medical devices by the competent department in the country/region where the applicants are located. (It is not required to submit such documents for innovative medical devices that have not been marketed abroad.) Furthermore, the instructions and labels of imported medical devices shall meet the relevant requirements.

10 General

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

Cloud-based services mainly involve issues such as cybersecurity and data protection. Users upload data to the cloud and cloud service providers will manage the data. This may cause issues such as cybersecurity and data breaches and information leakage.

In addition, medical and health data are required to be stored within the territory of China, and those that need to be provided overseas shall be subject to a safety assessment and review according to the relevant regulations. As for service providers who have established data centres in multiple jurisdictions, there may be a risk of illegal cross-border data transfer.

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

Non-healthcare companies which plan to independently and directly engage in the digital health industry should first obtain the qualification licence for the corresponding business according to law. For example, those intending to provide online consultation, paid medical information and other services and construct a medical big data cloud-based platform through medical websites and APPs, shall obtain the approval of regulatory agencies and the relevant qualification licences.

If non-healthcare companies such as Internet companies intend to engage in the digital healthcare industry by cooperating with medical institutions, they shall agree with the cooperative medical institutions in a written agreement on the methods of cooperation, the responsibilities and rights of each party in medical services, information security, privacy protection and other aspects.

If non-healthcare companies choose to develop and produce AI medical software, wearable medical devices and other products, they shall also comply with relevant regulatory requirements on medical devices and AI-aided diagnosis technologies.

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

Apart from business models, business prospects and other commercial factors, VC and PE investors should also pay

attention to key issues such as market access requirements for the industry that the target company falls into, the business qualification and business license, core technologies and key technicians, procedures for obtaining ownership of relevant intellectual property rights, hardware facilities and cybersecurity protection, etc.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Pursuant to the Measures for the Administration of the Clinical Application of Medical Technologies and relevant provisions, medical technologies in China are subject to a "categorised" regulation system. AI-aided diagnosis and AI-aided treatment fall within the scope of "restricted technology", and a medical institution intending to carry out the clinical application of such restricted technology shall conduct self-assessment according to the standards for the administration of the clinical application of medical technologies. A qualified institution may carry out clinical application and shall report to the health administrative department for filing. New medical technologies which have not been verified in clinical practice are considered to fall within the scope of "prohibitive technology" and cannot be used in clinical diagnosis and treatment.

The clinical adoption of digital health products which fall into the scope of medical devices shall go through approval or filing procedures according to the Administrative Measures on the Registration and Recordation of Medical Devices, the Measures for the Administration of the Clinical Use of Medical Devices and relevant provisions, and shall comply with the requirements in the aspects of clinical trial institutions, systems, procurement, operation management, and handling of safety involving the use of medical devices, failing which will result in administrative penalties from the competent authorities.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In China, there is no physician certification bodies that influence the clinical adoption of digital health solutions. The qualification licence and relevant requirements for physicians engaged in clinical adoption are mainly stipulated under the Physicians Law of the PRC, the Measures for the Administration of the Clinical Application of Medical Technologies, and the Measures for the Administration of the Clinical Use of Medical Devices and relevant provisions.

The China Medical Practitioner Association mainly performs the following duties: to implement industry management; formulate self-discipline rules; provide support such as legal assistance for medical practitioners; provide continuous education for medical practitioners; and organise academic meetings and seminars.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

In China, if patients have subscribed to or are covered by basic medical insurance, and the expenses of medical treatment items and medical service facilities are partially or completely covered by the basic medical insurance catalogue, the relevant expenses can be settled and reimbursed according to the medical service agreements signed between the government medical insurance agency and the designated medical insurance institutions. In addition, patients can purchase private insurance and be reimbursed for relevant medical expenses from private insurance companies.

After the promulgation of the Guiding Opinions of "Internet Plus" Medical Services on October 24, 2020, Internet Plus Medical Services was formally allowed under the medical insurance payment. The expenses of examination and prescription incurred from return visits in "Internet Plus Medical Services" designated medical insurance institutions by the insured in areas subject to overall planning can be reimbursed according to relevant regional medical insurance policies.

Cindy Hu focuses on areas such as corporate mergers & acquisitions, as well as corporate finance and compliance. She is deeply involved in the pharmaceutical and healthcare industry, and leads the pharmaceutical and healthcare team of E&C.
Cindy has routinely advised well-known Chinese state-owned and private enterprises, publicly listed companies, and private equity/venture capital funds in the area of pharmaceuticals and healthcare. She was recognised as one of the Top 15 M&A Lawyers by *ALB China*, as well as one of the Client Choice: Top 15 Compliance Versatile Practitioners by *LEGALBAND*. She was also endorsed as a Leading Lawyer in Corporate Mergers & Acquisitions by *Asialaw Profile* and *China's Top Lawyers* (Corporate and Mergers & Acquisitions) by *LEGALBAND* multiple times. Cindy is widely published both in China and internationally.

East & Concord Partners
20/F Landmark Building Tower 1, 8 Dongsanhuan Beilu
Chaoyang District
Beijing 100004
China

Tel: +86 10 6590 6639
Email: cindyhu@east-concord.com
URL: www.east-concord.com

Jason Gong is a partner in the Intellectual Property Department and a key member of the pharmaceutical and healthcare team of E&C. Gong's services cover various IP rights procurement and management, due diligence, enforcement, and anti-counterfeiting, including both non-contentious, such as patent/trademark prosecution, advising on patent validity and freedom-to-operate, infringement analysis, and consulting on patent portfolio, as well as contentious fields, such as patent validity proceedings, infringement litigation, customs protection and other administrative actions against infringers, and IP enforcement at fairs.
Jason has rich experience in IP protection for the chemical industry including pharmaceutical and life science. He represents foreign industry giants in pharmaceutical, agrochemical and refrigerant sections, and also local prestigious universities and academic centres. He frequently provides patent-focused advice for many bio-pharmaceutical companies and start-ups.

East & Concord Partners
20/F Landmark Building Tower 1, 8 Dongsanhuan Beilu
Chaoyang District
Beijing 100004
China

Tel: +86 10 6590 6639
Email jianhua_gong@east-concord.com
URL: www.east-concord.com

Jiaxin Yang is the backbone member of the pharmaceutical and healthcare team of E&C, with rich experience in mergers & acquisitions, compliance and risk control in the sector of healthcare. She regularly provides support and advice for well-known Chinese state-owned and private enterprises, foreign invested companies, as well as private equity funds on projects concerning stem cell research and development, digital health, wearable medical devices, cybersecurity and data protection.

East & Concord Partners
20/F Landmark Building Tower 1, 8 Dongsanhuan Beilu
Chaoyang District
Beijing 100004
China

Tel: +86 10 6510 7422
Email: yangjiaxin@east-concord.com
URL: www.east-concord.com

East & Concord Partners ("E&C") has a well-earned reputation as one of the largest and most comprehensive law firms in China. With more than 500 legal professionals, the firm advises multinational companies, publicly listed companies, privately owned companies, state-owned enterprises, foreign invested companies, government offices and public institutions on a wide range of areas. Headquartered in Beijing, the firm has seven offices strategically located throughout China. The firm has also established extensive cooperation with many well-known international law firms so as to satisfy the development need of the economic globalisation.
With nearly 30 years of experience, the firm has gained a leading position and earned clients' trust and recognition in areas including banking and finance, mergers & acquisitions, anti-dumping and anti-subsidy, pharmaceutical and healthcare, infrastructure and project financing, intellectual property, government legal affairs, cybersecurity and data protection, and dispute resolution.

www.east-concord.com

天達共和律師事務所
East & Concord Partners

France


Anne-France Moreau


Lorraine Maisnier-Boché


Caroline Noyrez

McDermott Will & Emery AARPI

1 Digital Health

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**) refers to "*telehealth*", which includes two forms of remote medical practice by means of information and communication technologies: **(i)** "*telemedicine*", "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-surveillance, tele-assistance and medical regulation (Art. R. 6316-1 *et seq.* FPHC); and **(ii)** "*telecare*", "which brings a patient together with one or more pharmacists or paramedic" (Art. L. 6316-2 FPHC). In practice, however, "digital health" encompasses various other products and services; although they are not strictly defined, they all refer to the digital revolution in healthcare to enable patients and HCPs to better monitor, manage and improve healthcare.

1.2 What are the key emerging digital health technologies in your jurisdiction?

Connected medical devices (**MD**), clinical support tools, telemedicine solutions and digital care products and tools are among the key emerging technologies in France. They include IT solutions intended for HCPs (e.g. clinical decision support, predictive analyses) and/or patients (e.g. teleconsultation platforms, online pharmacies). The French government demonstrated its commitment to foster the development of digital health technologies by launching a 2022 "My Health" plan notably aimed at accelerating the digitalisation of healthcare through the creation of Digital Health Space (*espace numérique de santé*) for patients.

1.3 What are the core legal issues in digital health for your jurisdiction?

Some of the core legal issues in digital health in France are the following:

- **Applicable Regime**: the regulatory status of a given digital health product will determine the relevant pre- and post-commercialisation considerations. Notably, the period for MD regulatory review has increased in Europe due to the coming into force of the new MD regulations (see question 2.6).
- **Regulatory evolution and reimbursement pathways**: regulations evolve rapidly and reimbursement pathways can be obscure. Close monitoring of institutional guidelines is key. For instance, telemedicine is effectively regulated since 2018 in France and the regulatory framework is expected to continue to evolve. Upcoming legislation will allow reimbursement of software-based telesurveillance for chronic diseases and will introduce an early reimbursement mechanism for innovative digital MDs used for telesurveillance.
- **Data protection**: digital health 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 as modified. French law also adds security and interoperability requirements specifically applicable to healthcare information systems (Art. L. 1111-8 and L. 1470-5 FPHC, see question 2.2).

1.4 What is the digital health market size for your jurisdiction?

According to a recent study by the Institut Montaigne, in association with McKinsey & Company, the digital health market could generate up to 22 billion euros per year in France. In particular, the proliferation of telemedicine has the potential to generate between 3.7 and 5.4 billion euros of value annually. The study also estimates the value of automation, via patient flow management tools or robotic logistics in hospitals for instance, between 2.4 and 3.4 billion euros per year. Finally, AI-based decision support tools could generate between 3.3 and 4.2 billion euros in annual value created.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

To our knowledge, the five largest digital health companies in France (by revenue) are Withings, Asten Santé (previously SADIR Assistance), Owkin, Kry and Lincor.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

European and French legislators have addressed many aspects of digital health, but there is no comprehensive regulatory scheme yet. Applicable rules range from relationships between supply chain operators, as well as HCPs and users, public health policy, and patients' rights in cross-border healthcare. At the French level, such regulations are mostly codified in the FPHC – e.g. anti-kickback and transparency provisions (Art. L.1453-1 *et seq.* FPHC), advertisement of MD (Art. 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 codes may also apply to specific aspects of healthcare (e.g. respect of the human body in the Civil Code (**FCC**), reimbursement schemes in the Social Security Code (**FSSC**), etc.). Finally, regulatory agencies play an important role in the construction and implementation of guidelines to improve the understanding of regulatory schemes by market actors.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Some other regulatory schemes that apply to digital health are the following:

- **Regulations on MD** (see question 2.6).
- **Regulations on anti-kickback and transparency requirements** (see question 2.1).
- **Regulation and reimbursement**: see question 1.3 and good practice guidelines set by regulatory agencies (see e.g. recent HAS guidelines on the reimbursement pathway for AI-based devices, on the assessment of mobile health apps or on classification of digital health solutions).
- **Regulations on electronic medical records**: health data security and interoperability requirements; upcoming implementation of a Digital Health Space (see question 1.2).
- **Regulations on data protection**: see section 4.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The line between wellness consumer devices (e.g. a diet app or sport assistant watch) and MDs with a medical purpose may be difficult to draw. There is no specific regulatory scheme for "consumer devices" as a standalone category. General regulations cover various aspects of consumer devices' life cycle – e.g. the French Consumer Code governs business-to-consumer relationships and defines defective product liability issues (Art. 1245 *et seq.* FCC). On the other hand, MDs with a medical purpose (including software) are subject to a specific regime (see question 2.6).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

Some of the principal regulatory authorities in France are the following:

- **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 care's quality, continuity and proximity.
- **National Agency for the Safety of Health Products (ANSM)**: 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 controls and sanctions data controllers and processors through the issuance of injunctions and fines.
- **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, including guidelines relating to digital health issues.
- **Regional Health Agencies (ARS)**: responsible for the regulation of healthcare provisions at a regional 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 standards regarding security and interoperability, as well as by developing national health software and projects.

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

Some of the key areas of enforcement regarding digital health in France are:

- **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 (including security) requirements may therefore result in severe sanctions, such as injunction to stop the processing or fines of up to EUR 20,000,000 or 4% of total worldwide annual turnover, which can be publicly issued.
- **Regulatory Requirements**: existing and future digital health solutions cover an extensive and highly diversified field, and market access 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 an MD (ANSM Decision 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)** the EU, Regulation (EU) 2017/745 on MD (**MDR**) or Regulation (EU) 2017/746 on *in vitro* diagnostic MD (**IVDR**) (directly enforceable in France and fully operative respectively from May 2021 and May 2022), and **(ii)** in France specifically, by the FPHC (see e.g. Art. L. 5213-1 *et seq.* FPHC on MD advertising). The new regulations broaden the range of technologies covered (e.g. devices aimed at medical prediction and prognosis are now expressly included), set forth a stricter classification regime (a new rule is notably introduced for standalone software MD, such as most health apps), and added rules on clinical performance evaluation of MDs.

Regulatory authorities have also issued guidelines tailored to software MD (e.g. MD Coordination Group of the European Commission guidelines on qualification and classification of such software in October 2019 MDCG 2019–11 and April 2020 MDCG 2020–5, 2020–6, 2020–7, and 2020–8; the HAS issued guidance on the assessment of connected MDs for reimbursement purposes).

2.7 What regulations apply to Artificial Intelligence/Machine Learning powered digital health devices or software solutions and their approval for clinical use?

AI and ML-powered MDs are subject to MD regulation, data protection regulations (GDPR and French regime on automated decision making) and bioethics rules. Other rules may apply as there is no comprehensive regulatory framework. The EU Commission has proposed harmonised rules regarding AI applications (the **AI Act**) which would pre-empt national regulatory frameworks, although monitoring and enforcement would remain the responsibility of Member States.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Depending on the digital health product or service, different legal regimes may apply, mainly the telehealth or online pharmacies regulatory requirements, and MD regulations. The COVID-19 pandemic has led to a proliferation of telemedicine platforms and upcoming legislative changes are expected and should be closely monitored (see question 1.3). Health data protection, security requirements, liability issues, and reimbursement of such products or services are also key.
- **Robotics**
  Several potential legal regimes may apply to robotics. Liability allocation is one issue, as well as the consideration of the regime of product responsibility.
- **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, MD 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 the use of AI to train them, requires strict compliance with data protection laws and security requirements and triggers some questions regarding algorithm transparency. Upcoming AI-based regulation should also be closely monitored.
- **Mobile Apps**
  Data protection and security requirements, specifically for health and/or monitoring apps, and the issue of liability, are key. Depending on the features, MD regulations may also apply.
- **Software as a Medical Device**
  MD and health data protection, including additional public health requirements regarding interoperability and security, will apply. Upcoming AI-based regulation should also be closely monitored. Proper liability allocation is key.
- **Clinical Decision Support Software**
  MD regulation will apply. Health data protection, including additional public health requirements regarding interoperability and security, will also apply. Proper liability allocation is key.
- **AI/ML powered digital health solutions**
  Training an AI- or ML-based health solution requires processing large amounts of personal data and of health data, triggering compliance requirements with data protection and security, specifically for sensitive data. Algorithm transparency and IT security must be ensured. MD regulations will also apply (see question 2.7).
- **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, MD regulations may also apply. Guidelines of the reimbursement of these devices should be closely monitored.
- **3D Printing/Bioprinting**
  3D bioprinting means the creation of living tissues via the additive manufacturing technology of 3D printing. MD regulation will likely apply, depending on the intended use.
- **Digital Therapeutics**
  Digital therapeutics are held to the same standards of evidence and regulatory oversight as traditional medical treatments (notably, either MD or drug regulation, or both). In addition, data protection and security requirements, as well as the issue of liability, are key.
- **Natural Language Processing**
  Natural language processing is at the crossroads of AI and personal data processing. Algorithm transparency, data protection compliance, and in some cases, medical device regulations are key. Depending on the support service, 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 offered, but the landscape is evolving rapidly. Online sale of medicines is, for example, subject to stringent requirements in France (only pharmacies may sell medicines; online sale is limited to over-the-counter drugs), but the COVID-19 pandemic has led to the proliferation of telemedicine platforms and to a variety of case law and governmental guidelines with it. Upcoming changes should be closely monitored.

Security and interoperability requirements are higher for digital health platform providers (e.g., if medical data are processed, they may only use the services of a certified health data hosting service provider (Art. L. 1111-8, FHPC) and must comply with security and interoperability standards, especially regarding data access (Art. L. 1470-5, FHPC). A certification scheme for interoperability has been considered but not yet implemented (Art. L. 1470-6, 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 lawfulness, fairness, transparency, proportionality, purpose limitation and data minimisation, and 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:

- maintain a record of processing activities under its responsibility;
- inform the individuals of the processing's existence; and
- ensure that the agreements entered into contain adequate provisions to properly determine the parties' capacities, 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 when based on a specific legal ground (e.g. express consent, or where necessary for purposes of care);
- health data processing must also be justified by a public interest and authorised by the French Data Protection Authority, unless it falls under exceptions; and
- organisational and technical security measures must be adapted to the level of data sensitivity (encryption, access monitoring, pseudonymisation or 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 conditions of implementation of its operations.

Some specific restrictions must be highlighted, for instance, prohibition to sell health data that are directly or indirectly identifiable (Art. L. 1111-8, VII, FPHC), or 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 essential;
- 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 parties' roles and responsibilities, 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 data controller's obligation to provide relevant information to the individuals, and, in some cases, to obtain their express consent, has an impact on contracts with individuals. Lack of such information may lead to the impossibility to use data in a lawful manner.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Data is an incredibly important business asset. It is thus highly important to negotiate adequate contractual provisions, in order for the capacities to be in line with the business needs to use data, to properly allocate responsibilities and to avoid sanctions (see question 4.3).

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 the 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 (see question 4.5) and to adequate security measures during transmission.

Personal data transfers to recipients located outside the EU, in a country that does not ensure an adequate level of protection, must be covered by appropriate safeguards, notably data transfer agreements (standard contractual clauses (**SCCs**) adopted by the EU Commission).

However, further to the *Schrems II* decision (CJEU, 16 July 2020, C-311/18, *Facebook Ireland* and *Schrems*), data controllers must conduct a risk assessment before using SCCs, and must also implement strong safeguards to ensure the protection of personal data from access by foreign authorities. In France, the French centralised public health database (the **Health Data Hub**) has been subject to various proceedings regarding potential transfers of health data to the US through the hosting service provider.

If data is covered by medical secrecy (Art. L. 1110-4 FHPC), a specific regime for "shared medical secrecy" generally requires patient consent to share its medical data with any party outside the healthcare team (Art. L. 1110-12 FHPC).

6 Intellectual Property

6.1 What is the scope of patent protection?

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 non-obvious "technical effect" and certain AI-related inventions directed to a technical subject-matter (e.g. a heart-monitoring apparatus' neural network detecting irregular heartbeats) may be patentable. Patents offer strong protection but are limited in scope (to the patent claims) and in duration (20 years). This protection also requires public disclosure of the invention as patent applications are published 18 months after being filed.

6.2 What is the scope of copyright protection?

Copyright protects an original work in a fixed form (Art. L.112-1, FIPC). Ideas, concepts or mathematical formula 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. The copyrights' holder benefits from economic rights and 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. Original works are protected without formalities from their day of creation, whatever their 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; **(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 (Arts L.151-1 to L.154-1 of the French Commercial Code). Trade secret protection may apply to corporate algorithms.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

There is no specific academic technology transfer rules scheme in France. Since 2019, France Biotech, an industry association, has been developing tools (negotiation process, templates, access to existing agreements) to facilitate and accelerate technology transfer and, in collaboration with BPI France, has begun to suggest improvements to the technology transfer process (see e.g. December 2020 report).

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, and 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).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

No. The European Patent Office has already refused patent applications designating an AI as inventor (January 2020).

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

Like in private transactions, industrial property rights allocation mostly depends on the specific contract executed between the government sponsor and the inventor(s). When the public authority plans to order products that are likely to be protected, particular attention must be paid to the proper management (e.g. method and duration of transfer/licence) of intellectual property rights in order to ensure that it will be able to use the products ordered in accordance with its needs. In order to help public and private entities in the negotiation and performance of their IP-related agreements, new standard intellectual property provisions, adapted to the different public contracts (e.g. IT contracts, collaboration contracts under which innovations may be developed, intellectual services contracts, etc.) entered into force on 1 April 2021 and shall be used by public authorities in the future.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The main consideration is to identify the applicable regulations and define a clear intellectual property scheme regarding the results generated during a partnership, depending on the allocation of responsibility between the parties during development. Academics often request joint ownership of results (independent of inventorship).

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

There are many considerations to assess: ensuring business continuity with respect to the product and/or process; warranties on the compliance/regulatory capabilities; cross-border concerns; and data breach indemnity.

8 AI and Machine Learning

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

Machine learning is proliferating in the digital health sector to assist HCPs' practice and research. AI can provide assistance in decision-making and make the decision itself, but only under very strict circumstances (notably to protect the subjects' data).

8.2 How is training data licensed?

Training data is protected by intellectual property rights as an entire database if it is original, or, if not, 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. Open databases may also be used without the need for a licence.

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 his or her employer (a company) if the employee acted within his or her duties or pursuant to the employer's instructions. The European Patent Office has already refused patent applications designating AIs as inventors (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 solutions?

- **Civil liability**: the producer of the device may be strictly liable for the provision of a defective product in case of harm to the user. Claims may also be brought against economic actors involved in manufacturing or distribution under fault-based regimes.
- **Criminal liability**: manufacturers, distributors, users and other actors involved in digital health may be liable for specific offences described in the FPHC, or ordinary offences (e.g. involuntary manslaughter).
- **Regulatory liability**: regulatory authorities may impose administrative sanctions to manufacturers that 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 (as modified) sets out the conditions under which a patient may receive medical care from a HCP located in another EU country – it covers healthcare costs, the prescription, and the delivery of medications and MD.
- **MDs and local representation**: to place an MD on the EU market, a non-EU manufacturer must designate an "*authorised representative*" in the EU (Art. 11, MDR).
- **Data transfer**: see question 5.2.

10 General

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

The key challenges with Cloud-based services for digital health lie in the setting up of sufficient security and governance mechanisms to enable users to demonstrate compliance with the strictest legal regime applicable to their operations.

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

The digital healthcare market is a highly regulated, complex sector to navigate through – solid knowledge of the industry (industrials, HCPs, regulators, patients, etc.) and the norms (regulatory barriers to market entry, liability exposure, etc.) is key.

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

A threshold consideration is whether the digital solution will provide the necessary features, functions and tools to meet the market needs, as well as comply with the abovementioned regulatory requirements.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Despite the growing number of digital health technologies, the evolution of methodologies to perform timely, cost-effective,

and robust assessments has not kept pace. Key barriers in France include the lack of comprehensive regulation and a sometimes obscure methodology for reimbursement of digital health solutions.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The SNITEM (*Syndicat National de l'Industrie des Technologies Médicales*) is the main representative (non-certifying) of the medical technology industry and is proactive in the field of MD regulation.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

They can be (by both), but a strict procedure applies. MDs must be CE-marked and any digital health solution must undergo a HAS assessment, be registered on a governmental list, and be prescribed by a HCP to be reimbursed in France.

Anne-France Moreau counsels companies founded on an 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 AARPI
23 rue de l'Université
Paris, 75007
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 programmes, international data transfers, marketing and profiling actions, sensitive data (e.g. personal health data), audits and security issues.

McDermott Will & Emery AARPI
23 rue de l'Université
Paris, 75007
France

Tel: +33 1 81 69 14 77
Email: lmaisnierboche@mwe.com
URL: www.mwe.com

Caroline Noyrez focuses her practice on transactional and regulatory matters in the field of pharmaceuticals, medical devices, biotechnologies and cosmetics. She assists French and foreign companies in the life sciences sector in their market access strategies and advises them on the preparation of their strategic contracts.

McDermott Will & Emery AARPI
23 rue de l'Université
Paris, 75007
France

Tel: +33 1 81 69 99 01
Email: cnoyrez@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 more than 20 locations on three continents – 13 US offices, seven European offices and now one office in Singapore – our team works seamlessly across practices, industries and geographies to deliver highly effective, and often unexpected solutions, that propel success. More than 1,200 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 and 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

Germany


Jana Grieb


Dr. Deniz Tschammler


Dr. Claus Färber


Steffen Woitz

McDermott Will & Emery Rechtsanwälte Steuerberater LLP

1 Digital Health

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

German law does not define "digital health" specifically. Generally, the term is interpreted broadly and includes, *inter alia*: (i) digital healthcare services, including telemedicine; (ii) medical software applications for smartphones; (iii) medical devices that include artificial intelligence; and (iv) other medical products that involve digital features, such as digital pills. Moreover, digital health is an umbrella term for the new markets in which the providers of the aforementioned products and services are active.

1.2 What are the key emerging digital health technologies in your jurisdiction?

Prescription and reimbursement of medical apps: A new system for the reimbursement of medical smartphone apps (*Digitale Gesundheitsanwendungen* – "DiGA") has recently been introduced under the statutory health insurance ("SHI") regime. The DiGA concept applies to apps that are CE-certified medical devices under MDR risk class I or IIa. In order to obtain reimbursement for a medical app, the manufacturer has to file an application with the German Federal Institute for Drugs and Medical Devices (*Bundesinstitut für Arzneimittel und Medizinprodukte* – "BfArM"). Once approved, the applicable reimbursement thresholds are determined by and negotiated with the Federal Association of the SHI Funds (*Spitzenverband Bund der Krankenkassen* – "SpiBu").

To obtain approval for reimbursement, the manufacturer must prove that the medical app meets the requirements for safety, functional capability and quality and that it complies with data protection requirements. Additionally, the manufacturer must show that the app has positive effects in patient care. These positive effects in patient care have to be established with a comparative study which demonstrates the advantages of using the app, as opposed to not using it. Such study must generally be retrospective. It does not have to be a genuine clinical trial. Valid concepts are epidemiological studies, or studies using methods from other scientific fields such as healthcare research.

At present, BfArM has approved 24 medical apps. The number of reimbursed medical apps will likely increase quickly as the system becomes more established.

Liberalisation of telemedicine: For many decades, telemedicine was largely restricted under German physicians' professional law. This had already started to change before the COVID-19 pandemic. In 2019, Germany had set the legal basis for telemedicine, including video consultation by physicians, and their coverage by private and public payers. The practical implementation of these laws has been accelerated significantly due to the pandemic and related restrictions on public life. The number of video consultations, online prescriptions and other types of remote patient treatment have meanwhile reached an all-time high. Physicians are now also allowed to issue a certificate for sick leave in a video consultation. Simultaneously, restrictions on the advertisement of telemedicine have, to some extent, been lifted.

Regardless of the above, telemedicine is still subject to numerous regulatory restrictions. According to German professional laws, remote treatment can only take place if, among other things, the use of the telecommunication medium is medically justifiable, i.e. no further medical examinations are necessary to obtain a direct and comprehensive picture of the patient and his or her disease. Moreover, telemedicine business models are subject to high data protection and IT security standards, as they involve the processing of a significant amount of health data.

1.3 What are the core legal issues in digital health for your jurisdiction?

Digital health trends are a major challenge for the German health sector, which is still characterised by many traditional rules and practices. The objective of the German government is to provide a functioning and secure healthcare telematics infrastructure that sets a digital framework and facilitates cooperation between various players in the domestic health markets. The telematics infrastructure seeks to achieve a balance between protecting the patients' fundamental rights of autonomy and confidentiality of their health data on the one hand and creating digital health services and a high level of work efficiency across the health sector on the other hand. One of the key issues of digital health is the handling of sensitive patient data, the extensive use of which has considerable value for research and development, but is at the same time limited by a number of local, national and EU regulations, including the General Data Protection Regulation ("GDPR").

1.4 What is the digital health market size for your jurisdiction?

The market for digital products and services in the healthcare sector is growing rapidly. There are various estimates on the market size, depending on the notion of digital health (as outlined under question 1.1 above) and the relevant key figures.

The size of the market is already today estimated to be in the tens of billions, with a strong upward trend.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

It is not possible to make a blanket statement in this regard. Many of the companies specialising in digital health are also active in other health or technology markets. As in other countries, the global tech companies such as Apple, Google, or IBM play a significant role in the digital health market. At the same time, university spin offs and other early stage companies are making their mark in this emerging sector as well. In the telemedicine sector, there are a number of promising platform operators that use their e-commerce and IT expertise to connect patients and physicians online.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Digital health products, including medical apps, often qualify as medical devices or *in vitro* diagnostics and, therefore, fall within the scope of Regulation 2017/745 on medical devices ("MDR") and Regulation 2017/746 on *in vitro* diagnostics ("IVDR"). As EU regulations, MDR and IVDR are directly applicable in Germany and do not have to be transposed into national law. The regulations are complemented by the German Act on the Implementation of EU Medical Devices Law (*Medizinprodukte-Durchführungsgesetz* – "MPDG").

Digital health services are subject to German healthcare regulations on the inpatient sector (e.g., hospitals and care homes) and outpatient sector (e.g., medical offices and home care providers). In these sectors, services are typically reserved for physicians or other healthcare professionals who may be entitled to provide healthcare services. Physicians are subject to the requirement of a German approbation or other permit to provide physician-only services, and bound by strict regulations under their professional codes.

Reimbursement of digital health products and services under the SHI regime is predominantly governed by the Fifth Book of the Social Insurance Code (*Fünftes Buch Sozialgesetzbuch*, "SGB V").

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The laws on data privacy, in particular Regulation 2016/679 (General Data Protection Regulation, "GDPR") and the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, "BDSG"), are particularly relevant to digital health products and services. It is key for any digital health products company to ensure that patient data are treated in line with these legal frameworks and protected against undue third-party access. Furthermore, depending on the respective health product or service, additional data protection regulations may apply, e.g., for the approval of medical apps or telemedicine services.

In Germany, the cooperation between the health industry and healthcare professionals ("HCP") is subject to various healthcare compliance regulations. Their purpose is to protect independent medical decisions of HCP, patient health and fair competition among healthcare providers. To this end, the regime in particular seeks to prevent any undue influence on HCP. The applicable healthcare compliance provisions are manifold and complex. They equally apply to any cooperation and business activities in the digital health sector.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

While there is no specific national scheme for "consumer healthcare devices", such products are subject to the laws and regulations described above. Under EU law, consumer products are generally subject to the General Product Safety Directive ("GPSD"). In the digital health sector, however, the GPSD is of minor relevance because the more specific medical device regulations, including the MDR, would typically apply instead of GPSD.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The German Federal Institute for Drugs and Medical Devices (*Bundesinstitut für Arzneimittel und Medizinprodukte* – "BfArM") regulates the market clearance and reimbursement for most digital health products. Market surveillance for medical devices, including medical apps, is carried out by supervisory authorities at regional level.

The Federal Association of the SHI Funds (*Spitzenverband Bund der Krankenkassen*, "SpiBu") and the Federal Assembly of the SHI and the Federal Panel Doctors' Association (*Gemeinsamer Bundesausschuss*, "G-BA") are the highest bodies of the SHI and involved in the majority of reimbursement decisions for digital health products and services.

Federal and Regional Data Protection Commissioners (*Datenschutzbeauftragte des Bundes und der Länder*) are responsible for the supervision of data protection efforts.

The Telematics Society *(Gesellschaft für Telematik* – "Gematik") was created specifically with regard to the task of developing a suitable and functioning healthcare telematics infrastructure, including an electronic patient health card, electronic patient files and e-prescriptions.

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

Compliance of medical device software ("MDSW") with the sector-specific laws and regulations is mainly supervised by regional market surveillance authorities and notified bodies. This includes regular and *ad hoc* audits. Legal violations by the manufacturer of MDSW may lead to reputational damage and qualify as an administrative or criminal offence. Depending on the circumstances of the individual case, they may result in fines, orders of corrective and preventive measures, or a market ban.

Where digital health products or services require the transfer and processing of personal health data, data protection authorities supervise the market as well. Failure to meet data protection requirements may result in severe sanctions, such as an injunction to stop the processing, and/or fines of up to EUR 20 million or 4 per cent of the total worldwide annual turnover, which can be publicly issued.

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

Medical device software ("MDSW") must bear a CE-mark in accordance with the MDR or IVDR. For that purpose, these products must undergo a conformity assessment procedure that, depending on the risk class, can be passed through by the manufacturer (self-certification) or requires the involvement of a notified body. Upon successful completion of the conformity assessment procedure, the CE-mark can be affixed to the MDSW product.

Before the MDR came into force, MDSW was generally classified under risk class I and subject to self-certification. Under the MDR, many MDSW are now subject to higher risk classes. Therefore, manufacturers must regularly obtain their CE certificates from notified bodies.

The transition scheme under the MDR allows for manufacturers of class I MDSW to benefit from a grace period. More specifically, they may continue to market their products under the previous MDD regime until 2024 if they have issued a declaration of conformity before the MDR has become applicable.

The Medical Devices Coordination Group ("MDCG") of the European Commission issued several guidelines on qualification and classification of MDSW.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

Germany has not enacted a specific law on Artificial Intelligence ("AI") so far. Products that include AI are subject to the same regulations as other products, including medical devices law and data protection, as well as cybersecurity regulations. As part of a medical device, AI software has to comply with the requirements of the MDR or IVDR.

The EU Commission published a draft regulation on AI on 21 April 2021. The regulation is expected to come into force no earlier than 2024. As things currently stand, the draft regulation shall not supersede to the EU medical devices regime but apply in parallel. AI systems shall be subject to regulatory requirements that increase with the level of risk associated to them. High-risk AI, including certain AI systems for medical technology, shall be subject to comprehensive legal obligations imposed on the respective operator.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Despite being liberalised to a substantial extent (see question 1.2 above), telemedicine and virtual care services are still considerably restricted. Remote treatment of patients must be medically justifiable, i.e. the treatment case may not require further medical examination in the doctor's practice. Moreover, telemedicine and virtual care services typically involve the collection and storage of sensitive patient data and, thus, require a comprehensive data protection compliance management.
- **Robotics**
  Robotics are machines that have the capacity to (partly) substitute healthcare professionals. Such machines will mostly qualify as medical devices (see question 2.6). 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 or smartglasses, often serve multiple purposes, and their primary purpose may not even be of a medical nature. However, if wearables come with health-related features, they might qualify as medical devices and require CE-certification.
- **Virtual Assistants (e.g. Alexa)**
  Virtual assistants (such as Amazon's Alexa, Microsoft's Cortana, or Apple's Siri) usually have not been designed with health-specific features and are thus not considered medical devices. Moreover, it would be challenging for third-party software that runs on these devices and has a medical purpose to meet the reliability standards required for medical device software.
- **Mobile Apps**
  Mobile apps that implement health-related features may be considered medical device software and, thus, may require CE-certification. Medical apps of MDR risk class I or IIa may be approved for reimbursement under the German Digital Care Act (*Digitale-Versorgungs-Gesetz*, "DVG") and the German Digital Health Applications Regulation (*Digital-Gesundheitsanwendungen-Verordnung*). They can then be prescribed by physicians and reimbursed by SHI funds, similar to medical aids.
- **Software as a Medical Device**
  As with mobile apps, other software that implement health-related features may equally qualify as medical device software (see above).
- **AI/ML powered digital health solutions**
  Digital health solutions powered by artificial intelligence and machine learning can be a powerful tool for medical diagnostics and monitoring.
  The training of neural networks and similar artificial intelligence/machine learning algorithms necessarily requires a large amount of personal health data that must be obtained in compliance with data protection laws. At the same time, the results are often not sufficiently protected by intellectual property rights (see question 8.3).
- **IoT and Connected Devices**
  Connected medical devices such as long-term EKG or blood pressure metres are subject to the MDR and thus require CE-certification. The processing of personal health data needs to comply with the GDPR. This usually means that the processing will be a service provided on behalf of a healthcare provider.
- **3D Printing/Bioprinting**
  3D printing and bioprinting can be used to manufacture prosthetics and tissues. In the future, this technology might even be used to create whole organs. The use of 3D templates for prosthetics and tissues also raises new intellectual property and licensing questions.
- **Digital Therapeutics**
  Digital therapeutics are treatment procedures based on digital technologies. Such technologies may, depending on their specific features, qualify as medical device software (see above).
- **Natural Language Processing**
  Natural Language Processing ("NLP") describes techniques and methods for automatic analysis and representation of human speech. The purpose of NLP is direct communication between humans and computers based on natural language (see 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?

Platforms that facilitate transactions between healthcare providers and patients are subject to the requirements of Regulation (EU) 2019/1150 (Platform-to-Business Regulation), which sets out minimum standards for terms and conditions, transparency and fairness. As such platforms do not qualify as licensed healthcare providers, they are not authorised to process health data under Article 9(2)(h) of the GDPR. Consequently, they will often need to obtain valid consent from end-users in order to perform their services.

As platforms handle health data, they are also subject to increased data security requirements. They may not rely on email, which is often unencrypted, but need to establish a more secure channel for communicating with patients instead.

4 Data Use

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

The use of personal data is governed by Regulation (EU) 2016/679 (General Data Protection Regulation – "GDPR"). Such data must be processed lawfully (i.e. on a legal basis), transparently and fairly. They must be collected for a specific purpose (purpose limitation), limited to what is necessary (data minimisation), be accurate, be kept only as long as necessary (storage limitation) and finally be kept securely (integrity and confidentiality) (Article 5(1) GDPR).

Health data is a special category of personal data. Its collection and further processing is generally prohibited unless a special exemption applies (Article 9 GDPR).

In addition to the requirements of the GDPR, the unauthorised disclosure of personal secrets of patients by healthcare professionals and their auxiliaries is subject to criminal liability under Sections 203 and 204 of the German Criminal Code (*Strafgesetzbuch* – "StGB").

For connected medical devices and other equipment, the Telecommunication-Telemedia Data Protection Act (*Telekommunikation-Telemedien-Datenschutzgesetz* – "TTDSG"), which transposes certain parts of Directive 2002/58/EC, imposes additional restrictions on remote access to data, even if it is not personal data.

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

The GDPR sets out different requirements for health data, depending on the nature of the entities involved and the purposes for which personal data is processed.

Licensed healthcare professionals are permitted to process special categories of personal data for the purpose of occupational and preventive medicine, diagnosis and treatment (Article 9(2)(h) GDPR). This covers laboratories and other healthcare professionals that cooperate with physicians, as well as medical and non-medical service providers acting on behalf of these professionals, and organisations that manage insurances and social security systems.

Research organisations, conversely, may rely on a permission to process personal data for scientific and historical research purposes under Article 9(2)(j) GDPR and Section 27 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz* – "BDSG").

For private organisations that are neither involved in the provision of healthcare nor in scientific research, the use of health data is more challenging. In many cases, such organisations need to obtain explicit consent as set out in Article 9(2)(a) GDPR, as no other exception from the ban on the processing of special categories of personal data applies. This includes suppliers of medical equipment or diagnostic services that wish to re-use personal data for their own purposes, such as product improvements, as well as entities that provide health-related products and services, such as vendors of wearables that record health data, or digital platforms that facilitate finding the best doctor who is an expert for specific ailments.

4.3 Which key regulatory requirements apply?

Under the GDPR, every entity responsible for the processing of personal data (data controller) is subject to transparency and documentation obligations. In particular, the data controller needs to:

- inform the individuals (data subjects) how their data is processed;
- maintain a record of processing activities; and
- conduct data protection impact assessments ("DPIA") and possibly consult with the competent authority prior to certain risky types of data processing – this will often apply to digital health applications which involve sensitive health data and new technologies.

Under the BDSG, an entity is required to appoint a data protection officer if it employs 20 or more persons with the processing of personal data, or if it needs to conduct a DPIA. Hence, digital health providers in Germany will usually require a DPO.

Healthcare professionals are also required to take additional measures to ensure that their staff and service providers are warned of their potential criminal liability and thus maintain confidentiality.

4.4 Do the regulations define the scope of data use?

Under the GDPR, the scope of data use is limited by the purpose for which the data was originally collected, and the legal basis used.

For health data in particular, the exceptions from the ban on the processing of special categories of data only apply to certain purposes. By way of example, healthcare professionals can use health data for the provision of medical services and related administrative purposes. However, if they exceed this scope – e.g., if they want to anonymise data to share it with the vendor of their equipment – they will need to look at a different exception. This often means that they need to obtain consent from their patients.

4.5 What are the key contractual considerations?

Regarding compliance with the GDPR, one of the key considerations is identifying the roles of the parties in relation to the processing of personal data:

- if an entity (processor) processes personal data on behalf of another (controller), a data processing agreement is required under Article 28 GDPR;

- if two entities are jointly responsible for the processing of personal data, they need to enter into a joint controller agreement under Article 26 GDPR; and
- between independent controllers, the GDPR does not directly require specific contractual provisions. However, the parties may want to restrict the re-use of data in order to minimise the risk on non-compliance with the GDPR.

Liability and indemnification obligations are two of the key considerations for every contract. For the use of health data, this is amplified due to the potential for high fines under the GDPR.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

German law does not generally provide for ownership in data as intellectual property or otherwise. Data can only be protected as part of a database under the *sui generis* database protection rights set out in Sections 87a *et seq.* of the German Copyright Act (*Urheberrechtsgesetz* – "UrhG"), which transposes Directive 96/9/EC. This protection, however, only comes into play if there was a substantial investment in the acquisition, verification or presentation of the contents of such database. The investment must be specific to the creation of the database. Efforts undertaken to collect data for other commercial purposes, such as providing healthcare services or developing medical software, will not be considered.

Failing a protection as a database, data can only be partially protected as a trade secret under the German Trade Secret Act (*Geschäftsgeheimnisgesetz* – "GeschGehG"), which transposes Directive (EU) 2016/943. For this protection to apply, adequate measures against unauthorised access must be taken, e.g. including non-disclosure agreements with any person with whom the data is shared.

Often, the ownership of the data is overshadowed by the rights of the patient or other data subjects under the GDPR. If the collection or processing of personal data is based on consent (as opposed to, e.g., the research exemption), this consent can be revoked at any time, and the data subsequently needs to be deleted. This usually means that data ownership is not the primary concern, provided that data is not aggregated or otherwise anonymised.

5 Data Sharing

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

Under the GDPR, there must be a legal basis for sharing personal data. In addition, the purpose for which this personal data is shared needs to be compatible with the purpose for which it was originally collected. In digital health markets, this often means that the healthcare professional collecting health and other personal data for purposes of diagnosis and treatment needs to obtain explicit consent from his or her patients in order to share data for other reasons, such as research or product improvement. This applies even when the professional aggregates or anonymises the data before sharing, as this preparation of data is already a processing activity outside the scope of the provision of healthcare.

When sharing data outside the EU, the GDPR imposes additional restrictions to ensure that the personal data remains adequately protected. If the target jurisdiction is not subject to an adequacy decision of the European Commission, adequacy must be ensured through effective contractual undertakings. For transfers to the United States, in particular, a recent decision of the Court of Justice of the EU (16 July 2020, C-311/18 – Schrems II) indicates that such contractual undertakings would not be effective and need to be supplemented with additional measures.

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

The GDPR sets out different requirements for health data depending on the nature of the entities sending and receiving the data.

Sharing data between healthcare professionals for the purposes of diagnosis or treatment is usually covered by an exception stipulated in Article 9(2)(h) of the GDPR. Similarly, professionals can share information with the health insurance for the purposes of billing under this exception. However, professional secrecy must be taken into account, and it must be ensured patients' secrets will only be shared with other persons subject to professional secrecy or written confidentiality undertakings.

In order to be able to share data with research organisations, one might rely on the permission to process special categories of personal data for scientific and historical research purposes under Article 9(2)(j) GDPR and Section 27 of the German Federal Data Protection Act ("BDSG").

Public healthcare providers (e.g., a municipal hospital) and research organisations (e.g., a state university) may be subject to additional restrictions from state data protection laws and governmental policies when sharing health data.

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

When sharing personal data, one of the key requirements is ensuring that there is a legal basis for the disclosure of personal data. For health data in particular, one of the exceptions set out in Article 9(2) GDPR needs to apply. In many cases, this requires obtaining the patient's or data subject's consent. For this consent to be valid, the data subject needs to be informed how their personal data will be used, and with whom it will be shared.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patent protection is granted – upon application – for any invention having a technical character, if it is new, involves an "inventive step" and is suitable for industrial application. In digital health markets, the core technology (e.g., sensors and hardware) is generally patentable, even if patents remain mostly used in this rapidly developing environment. The number of worldwide Internet of Things ("IoT") patent applications increased substantially to over 130,000 per year; the health sector is contributing significantly to this development.

6.2 What is the scope of copyright protection?

Copyright law has the purpose of granting exclusive, non-registered rights to the author or creator of the original non-technical work. The work can also take the form of

a computer program, e.g., a statement, program language or mathematical 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. Data created by digital health programs, however, can never be subject to copyright, because they are 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 a useful 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 secret once placed on the market. In order to actually maintain secrecy, companies must – in accordance with the new German Trade Secret Act (*Geschäftsgeheimnisgesetz* – "GeschGehG") – 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 it does not cover generated data.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

Academic technology transfer from university employees to their university employer is subject to certain employee privileges under the German law on employee inventions because of the freedom of teaching and research. As opposed to other employees, a university employee does not have an obligation to report or to disclose a service invention. If a university employee wishes to disclose his or her invention, he or she must notify the university employer of the invention. If a university claims a service invention which was disclosed by its employee, the inventor retains a non-exclusive right to use the service invention within the scope of his or her teaching and research activities. If the university exploits the invention, the amount of the remuneration is 30 per cent of the income generated by the exploitation. This percentage is much higher than the employee invention remuneration of a normal employee.

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

In the healthcare sector, the main question is whether intellectual property protection is available for software inventions, e.g., medical device software ("MDSW"). If MDSW 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 same rules apply to copyright, since the underlying concept is never fully protected. Trade secret protection for medical device software is only possible under the restrictions described in question 6.3.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

So far, an AI device has not been named as the inventor of a patent in Germany. Several applications for the registration of patents "invented" by an AI device have already been rejected in Germany.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The contractor may be obliged to grant a back licence under the EU, federal or state level funding regulations on publicly funded research and development projects. In general, public grants contain ancillary provisions that must be fulfilled to avoid a possible revocation of the funding decision and the reimbursement of the grant. In addition to exercise and exploitation obligations, the funding conditions include obligations to grant access and utilisation rights in favour of the funding agency as well as the subcontractors. The Subsidiary Conditions for Grants from the German Federal Ministry of Research and Education (*Bundesministerium für Bildung und Forschung* – "BMBF") for Research and Development Projects ("NKBF 98"), e.g., require that the results be made available to research and teaching in Germany free of charge.

In addition, inventions which are the result of publicly financed research & development or innovation activities are subject to the EU regulatory framework for state aids according to Articles 107 and 108 of the Treaty on the Functioning of the European Union (TFEU) and the corresponding EU Commission Communication on Research, Development and Innovation (2014/C 198/10). Under these rules, any transfer of funded inventions to commercial undertakings must be remunerated at the market price.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Collaborations in the digital health sector are mostly subject to extensive contractual agreements, that aim at a fair balance of IP rights allocation and commercialisation rights on the one hand, and regulatory responsibilities and product liability on the other hand.

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

When cooperating with healthcare companies or healthcare professionals, non-healthcare companies should avoid granting any benefits, both unilaterally (e.g., gifts) and as part of (bilateral or multilateral) cooperation agreements. In such agreements, therefore, services and consideration must be equivalent, i.e. any remuneration must be at arm's length (principle of equivalence).

When granting benefits, companies should avoid the impression that there are any commercial expectations associated with such benefits. In particular, benefits must not create an incentive for the healthcare company or healthcare professional to make a certain procurement or therapy decision. In other

words, if companies grant any benefits, this should be for legitimate objective reasons and kept separate from other businesses or commercial interests (principle of separation).

In the event of a cooperation with healthcare companies or healthcare professionals, any details of such cooperation should be agreed upon in written form and as transparently as possible. In particular, companies should avoid any (additional) verbal agreements or other non-transparent arrangements as these give the impression of secrecy (principles of transparency and documentation).

8 AI and Machine Learning

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

Machine learning usually refers to the use of an algorithm ("neural network") that is trained with representative input data (e.g., images or sensor information) and the desired output. The algorithm is thus trained to recognise patterns in input data and to produce a certain output.

Machine learning can be a powerful tool for diagnostic purposes to assist healthcare professionals and to monitor the success of patient treatment. It can also be used for the early detection of potential health issues, even in consumer devices such as smartwatches or smartphones.

8.2 How is training data licensed?

Training data is often protected under the *sui generis* database protection rights set out in Sections 87a *et seq.* of the German Copyright Act (*Urheberrechtsgesetz* – "UrhG"), which transposes Directive 96/9/EC on the legal protection of databases. In this case, it can be licensed in the same manner as other intellectual property.

Licensing training data will often be challenging, as it includes personal health data, which is under strict protection under the GDPR regime. Consequently, training data can often be licensed in anonymised form only. One of the main considerations is how to ensure that it will not be possible to re-identify individuals.

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

As a general rule, intellectual property can only be produced and owned by human beings, not by machines. For this reason, improvements made without active human involvement do not fall under the protection of most intellectual property rights.

In some cases, the results may be protected by *sui generis* database protection rights (see question 8.2 above). Unlike other types of intellectual property, this protection only requires a substantial investment, but not necessarily an intellectual achievement.

Furthermore, the improvements might be protected as trade secrets of the entity that made them.

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

The main consideration is the ownership and/or access to the results of the training, i.e. the trained algorithm. As the algorithm may often not be protected by intellectual property rights (see question 8.3), it is crucial to clearly define the rights and obligations of each party with respect to its further use in the commercial agreement.

As training data will often include personal health information, it is also important to agree on liability and indemnification provisions in case the use of the licensed data turns out to be a violation of the GDPR. This could, e.g., be the case if the consent given by the patients is invalid or if the data has not been properly anonymised.

9 Liability

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

Besides regulatory responsibility and potential criminal charges, civil law liability plays a significant role in digital health markets. Under German law, there is contractual liability on the one hand, and tort liability under the German Civil Code (*Bürgerliches Gesetzbuch* – "BGB"), as well as product liability under the Product Liability Act (*Produkthaftungsgesetz* – "ProdHG") that each cannot be restricted by a contract on the other hand. Medical device software is subject to liability under the ProdHG, even if not offered in a material object as data carrier.

9.2 What cross-border considerations are there?

Liability rules are predominantly subject to Member State law. With regard to cross-border matters, the EU Regulation 593/2008 ("Rome I Regulation") and the EU Regulation 864/2007 ("Rome II Regulation") regulate the applicable national legislation. Under Art. 4 of the Rome II Regulation, applicable law is determined on the basis of where the damage has occurred, irrespective of the country in which the act that has caused the damage took place. There are two general exemptions from this rule: (i) if the parties reside in the same country, the law of that country shall apply; or (ii) if a tort is apparently more closely connected to a country other than where the damage occurred or where both parties live – in that case, the law of that other country is applicable. Furthermore, exemptions apply with regard to certain types of liability. For product liability, specific rules apply according to Art. 5 of the Rome II regulation. Here, the place where the product was acquired can become decisive. Under the Rome I Regulation, parties are under certain conditions allowed to determine the applicable law by contract. In the absence of a contractual choice of law, with regard to services, the law of the service provider's residence is applicable. However, there are exemptions to this rule with regard to consumer contracts, where generally the law of the consumer's country of residence is applicable.

Given that cross-border liability cases can result in severe legal consequences and significant loss of reputation in all countries concerned, cross-border digital health companies should adopt a global compliance regime and establish an organisation that takes into account the specific legal requirements and pitfalls of each national legal system concerned.

10 General

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

Healthcare organisations that transfer IT operations to clouds are facing, *inter alia*, technical and legal challenges. Security and confidentiality are key aspects for a wide-scale offering and use of cloud-based services. To reduce the risk of cyber-attacks and

the loss of personal data, healthcare organisations must ensure a safe system to transfer, maintain and receive health information. Confidentiality can be achieved by access control and by using encryption techniques. Healthcare data may be exchanged only in pseudonymised or even anonymous form. In certain legal regimes, it may be obligatory that cloud-based services are carried out in Germany or the EU at the very least.

In Germany, the legislator enacted the Health IT Interoperability Governance Ordinance (*Gesundheits- IT -Interoperabilitäts-Governance-Verordnung* – "GIGV") to ensure the secure and fast cloud-based transfer of patient data.

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

As shown above, digital health products and services are strictly regulated and under a high level of surveillance. To offer such products and services on the market, companies must establish a comprehensive compliance organisation, including to meet the various regulatory, data protection and healthcare compliance requirements.

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

There are restrictions to corporate ownership of certain healthcare service providers. While there are no ownership restrictions for hospitals, such restrictions exist with regard to physician practices and medical care centres (*Medizinische Versorgungszentren* – "MVZ"). As hospitals are entitled to hold MVZ, this is an option for corporate entities to indirectly operate MVZ and thereby employ physicians.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key barriers include high-market entry, reimbursement and compliance requirements. The market entry of medical device software is largely restricted by certification procedures under the new MDR and IVDR regimes that often require the involvement of notified bodies. However, as the new regulations maintain the general certification system and do not introduce a genuine approval requirement for medical device software (unlike for drugs), they are still regarded as an efficient market clearance system. On the reimbursement side, while it may be difficult and time-consuming to convince SHI funds of new and innovative digital health products or services, recent legal developments have facilitated reimbursement, e.g., in the area of medical app prescriptions. Still, companies entering the German digital health markets must observe a number of regulations, including with respect to the processing and use of health data and cooperation with healthcare companies or healthcare professionals. In clinics, many healthcare services are still reserved to the physician by statutory laws and, hence, not or only partly replaceable by digital health solutions.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The German Physicians' Chamber (*Bundesärztekammer* – "BÄK") supervises all physicians practicing in Germany. The Panel Doctors' Associations (*Kassenärztliche Vereinigungen* – "KV") supervise doctors that are entitled to provide healthcare services reimbursed under the SHI regime. Medical societies (*Fachgesellschaften*) issue guidelines that determine whether a treatment is considered state of the art.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

In Germany, medical apps have recently become subject to a general reimbursement scheme (see question 1.2 above). Besides that, reimbursement depends on the legal status of the respective digital health product or service. Medical devices may be reimbursable as medical aids (*Hilfsmittel*), or – on certain cases after testing periods – as new treatment methods. Digital healthcare services provided by physicians are reimbursed in the same manner as traditional physician services: their reimbursement in the outpatient sector in the SHI is subject to the Uniform Assessment Measure, (*Einheitlicher Bewertungsmaßstab*, "EBM"). New digital health products or services must be listed in EBM in order to obtain reimbursement. Where such listing takes too long, companies still have the option to enter into reimbursement negotiations with individual SHI funds.

Jana Grieb, Counsel, based in Munich, specialises in healthcare and life sciences, with a particular focus on the pharmaceutical and medical device 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.

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 322
Email: jgrieb@mwe.com
URL: www.mwe.com

Dr. Deniz Tschammler, Partner, based in Munich, specialises in complex legal, commercial and strategic projects in the health and life sciences sector. He advises on transactions and collaborations, disputes in and out of court, market entry and reimbursement pathways, as well as data protection and other compliance challenges of an increasingly digitised industry. His clients involve global pharmaceutical companies and medical device manufacturers, early-stage companies with a focus on innovative health products and disruptive business models, as well as investors in German and European health markets.

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 326
Email: dtschammler@mwe.com
URL: www.mwe.com

Dr. Claus Färber, Counsel, based in Munich, represents clients on all legal matters related to the telecommunications, media and information technology (IT) industries and has extensive experience advising international clients across industries on European data protection matters. Claus drafts and negotiates software licence agreements, other IT contracts, business process outsourcing agreements and significant procurement agreements in the telecommunications, e-commerce and IT industry, and assists with significant litigation in these industries. His transactional experience includes major cooperation and framework agreements, such as internet access in aircraft, WiFi hotspots, roaming, cloud platforms and machine-to-machine communications (M2M).

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 151
Email: cfaerber@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.

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 181
Email: swoitz@mwe.com
URL: www.mwe.com

India


Manisha Singh


Pankaj Musyuni

LexOrbis

1 Digital Health

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

In its broadest definition, "digital health" refers to the use of digital technologies to improve healthcare efficiency and give patients more personalised treatment. In India, the terms "digital health" and "digital medicine" are not defined. The Digital Information Security in Healthcare Act of 2018 (the DISHA Bill), on the other hand, defines "digital health data" as an electronic record of health-related information about an individual, including information about: an individual's physical and mental health condition; health services provided to an individual; the donation of any body part or bodily substance by an individual; and testing and examination data of an individual.

It is also worth noting that the Indian government issued the Telemedicine Practice Guidelines (TPG) in March 2020, which adopt the World Health Organization's (WHO) definition of telemedicine as "the delivery of healthcare services by all healthcare professionals, using information and communication technologies, where distance is a critical factor".

Using information and communication technology in healthcare, a variety of tools and services are used to prevent, minimise, treat, and monitor disease patterns. The concept of digital health is exemplified by the application of genetics and digital technologies to detect disease early. The Ministry of Health and Family Welfare (MoHFW) of the Indian government oversees and regulates this industry.

1.2 What are the key emerging digital health technologies in your jurisdiction?

Telemedicine, mobile health, health and wellness applications, medical imaging, big data, the Internet of Medical Things (IoMT), robot-assisted surgery, self-monitoring healthcare devices, Electronic Health Records (EHR), Health Service Aggregation, targeted advertising, personal genomics, personalised medicine, e-pharmacies, cloud computing, and Artificial Intelligence (AI) are some of the key emerging technologies in India's digital healthcare system.

1.3 What are the core legal issues in digital health for your jurisdiction?

When it comes to patient-provider discussions concerning health conditions and recommendations, data security is critical. The Information Technology Act of 2000, the Data Protection Rules of 2011, and the Intermediaries Guidelines of 2011 are all available to meet this demand, but no standards have been devised to mandate the implementation of data protection and security due to their rigorous adherence. Furthermore, as the number of digital and other new technologies in the healthcare industry develops, concerns regarding patient privacy and data security are growing. Even while most data collection, storage, and use by healthcare providers would be consistent with India's present data privacy rules, there are substantial worries regarding data abuse and privacy obligations. The absence of sufficient education and training for personnel responsible for collecting, processing, and handling patient data on the digital health platform is another element contributing to the current predicament. The Personal Data Protection Bill, 2019, was introduced in the Lok Sabha on December 11th, 2019. The bill creates the Data Protection Authority, whose goal is to protect people's personal data. In addition, the lack of a comparable law is a major concern. The DISHA Bill has yet to be signed into law. The DISHA Bill, which intends to prevent health-related information from being shared with other parties, will create national and state health agencies. The MoHFW has also established a National Digital Health Mission-related Health Data Management Policy to ensure that individuals' digital health data privacy is maintained.

1.4 What is the digital health market size for your jurisdiction?

India's digital adoption increased by more than 95% between 2015 and 2021, making it one of the world's fastest-growing digital economies at this time. To increase quality and access to services, the Indian healthcare sector has embraced digital change. India's digital healthcare business is expected to develop at a CAGR of 27.41 per cent to USD 485.43 billion by 2024.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

Apollo Hospitals Enterprises Ltd., Aster DM Healthcare Ltd., Dr. Lal PathLabs Ltd., Fortis Healthcare Ltd., and Healthcare Global Enterprises Ltd. are the top five healthcare corporations. In addition, among the top five Indian health-tech start-ups are Cure.Fit, DocsApp, Forus Health, HealthPlix, and Innovaccer.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The usage of digital health in India is governed by a few laws, guidelines, and standards. Several regulations are universally applicable to digital health technology, even though each digital health tool/business model is governed independently. In this regard, the Information Technology Act of 2000, the Information Technology (Reasonable security practises and procedures and sensitive personal data or information) Rules of 2011 (SPDI Rules), and the Information Technology (Intermediaries Guidelines) Rules of 2011 (Intermediaries Guidelines) are all relevant. The IT Act, SPDI Rules, and Intermediary Guidelines are all part of India's general data protection framework. Online transactions and the transfer of electronic data are now allowed thanks to the IT Act. The IT Act regulates a wide range of online activities, including the authentication of digital signatures and the legal validity of electronic records. The IT Act addresses cybercrime like hacking and denial of service attacks, as well as other types of cybercrime.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The Information Technology Act of 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011, which provide some protection for the collection, disclosure, and transfer of sensitive personal data such as medical records and history, govern the current legal framework for e-health protection in India. Legislation, on the other hand, has lagged in technological advances and fails to address several critical issues. As a result, the government passed DISHA as well as the 2019 Personal Data Protection Bill (PDP Bill).

The PDP Bill, which governs personal data management in India, applies to the Indian government, any Indian corporation, any Indian citizen, and any legal organisation established or established under Indian law. The rule applies to foreign businesses that process personal data while conducting business in India, as well as any systematic activity of delivering items or services to data principals within India's territory, or any activity involving data principal profiling.

As a result, medical institutions and healthcare providers in India are increasingly storing patient information in electronic medical records (EMRs) and electronic health records (EHRs). According to the Clinical Establishments (Registration and Regulation) Act 2010, each clinical institution must keep an EMR for each patient to be registered and maintained. EHR Standards were first introduced by the Ministry of Health and Family Welfare in 2013, and they were amended and released in December 2016.

EHR Standards are a set of global standards that healthcare providers can use to create and manage electronic health records. Some of the key ongoing digital health initiatives being implemented by the 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), and Online Registration System.

These programs are well established in the medical field and continue to generate large amounts of data that can be used to benefit the public. States are subsidised under the National Health Mission (NHM) for connected services such as Telemedicine, Tele-Radiology, Tele-Oncology, Tele-Ophthalmology, and Hospital Information Systems, as health is a state concern.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Typically, the Designs Act of 2000 protects consumer devices. Only features of shapes, configurations, patterns, ornaments, or the composition of lines or colours that are applied to an "article" have been defined as a "design". The two major components of digital health that would necessitate design protection are the Graphical User Interface (GUI) of applications and the design of the devices. The Designs Act, specifically Article 14-04 of the Design Rules, 2001, which covers "Screen Displays and Icons", may protect GUI. Furthermore, the CDSCO has published a draft risk classification list for medical devices regulated under the New Definition Notification. The risk classification list classifies medical devices into 24 broad categories (as defined by international classification standards), with standalone software classified as a separate category.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The Central Drug Standards Control Organisation (CDSCO) is the primary regulatory body in charge of enforcing the provisions of the "Drugs and Cosmetics Act, 1940" and "Rules thereunder". The Medical Council of India also regulates the practise of medicine. In addition, the Office of the Controller General of Patents, Designs, and Trade Marks (CGPTDM) oversees intellectual property protection, while the Copyright Office oversees copyright. Both are part of the Department for Promotion of Industry and Internal Trade (DPIIT). Furthermore, the Indian Council of Medical Research (ICMR) has played a key role in encouraging research in support of MoHFW's National Digital Health Blueprint (NDHB).

The following important acts normally control the legal and regulatory framework:

- The Information Technology Act of 2000, the Information Technology (reasonable security practises and procedures and sensitive personal data or information) Rules, 2011, and the Information Technology Rules, 2011 are all part of the Information Technology Act of 2000.
- Regulations for Other Service Providers under the New Telecom Policy of 1999.
- The 1940 Drugs and Cosmetics Act as well as the 1945 Drugs and Cosmetics Rules.
- The Indian Medical Council Act, 1956, and the Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002, are the laws that govern the Indian Medical Council.
- The Drugs and Magic Remedies Act of 1954, as well as the Drugs and Magic Remedies Rules of 1955, govern the use of drugs and magic remedies.
- Telecom:CommercialCommunicationCustomerPreference Regulations, 2010 and Unsolicited Commercial Communications Regulations, 2007.
- The Clinical Establishments Act, 2010.

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

Standards that maintain the security, confidentiality, and privacy of patients' health and records are key areas for enforcement. Due to protected private health information and records used only for data interpretation for market analysis, marketing, and regulatory sharing, data protection and infringement are important for enforcement.

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

The Central Drug Standards Control Organization (CDSCO), which itself is part of the Directorate General of Health Services (Ministry of Health & Family Welfare), is the primary regulatory authority in India for medical devices and diagnostics. The CDSCO's top official is the Drug Controller General of India (DCGI). The DCGI oversees approving the production of certain drugs (vaccines, large volume parenteral, blood products, r-DNA derived products), medical devices and new drugs. The manufacture, import, sale, and distribution of medical devices in India are governed by the Drugs and Cosmetics Act and Rules (DCA). Only notified medical devices are currently regulated as 'drugs' in India under the Drugs and Cosmetics Act 1940 and Rules 1945 made thereunder:

(i) substances used for *in vitro* diagnosis and surgical dressings, surgical bandages, surgical staples, surgical sutures, ligatures, blood and blood component collection bags with or without anticoagulant covered under sub-clause (i);

(ii) substances including mechanical contraceptives (condoms, intrauterine devices, tubal rings), disinfectants and insecticides notified under sub-clause (ii); and

(iii) devices notified from time to time under sub-clause (iv), of clause (b) of Section 3 of the Drugs and Cosmetics Act, 1940.

2.7 What regulations apply to Artificial Intelligence/Machine Learning powered digital health devices or software solutions and their approval for clinical use?

At the moment there are no formal regulations.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - A. Adoption of technology.
  - B. Evidence.
  - C. Technical training.
  - D. Record keeping and data management.
- **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.
  - C. Data management and privacy.
- **Software as a Medical Device**
  - A. Software development lifecycle.
  - B. Product safety and security.
  - C. Data collection, analysis and privacy.
- **Clinical Decision Support Software**
  - A. Development lifecycle.
  - B. Product safety and accuracy.
  - C. Data analysis.
- **AI/ML powered digital health solutions**
  - A. Lack of precision.
  - B. Lack of interpretation.
  - C. Irregularity in analytics.
  - D. Reliance.
  - E. Transparency and governance.
  - F. Long-term cost.
- **IoT and Connected Devices**
  - A. Compatibility of operating systems.
  - B. Identification and authentication of devices and technologies.
  - C. Integration of Internet of Things (IoT) products and platforms.
  - D. Connectivity.
  - E. Data analytics, security, and privacy.
  - F. Consumer awareness.
- **3D Printing/Bioprinting**
  - A. Piracy.
  - B. Misinterpretation of results.
  - C. Lack of training skills.
- **Digital Therapeutics**
  - A. Lack of accuracy.
  - B. Lack of interpretation and understanding.
- **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?

Understanding and maintaining the transitional phase of implementing new technologies is usually the primary issue for digital platform providers. As a result, some of the primary concerns for digital platform providers are: replacing and improving the existing IT system; competence training for employees, as well as understanding the importance of customer demand from the market and in line supply; and leadership.

4 Data Use

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

Data privacy is a major concern in the use and implementation of personal data. In 2013, the first Electronic Health Record Standards (EHR Standards) for India were proposed. They were chosen from among the best available, previously used international EHR standards, with an eye toward acceptance and relevance in India. As a result, the EHR Standards 2016 document was alerted and posted in IT systems across the country for adoption by healthcare institutions and providers. The Ministry of Health and Family Welfare aided its adoption by making standards such as the Systematised Nomenclature

of Medicine Clinical Terminology (SNOMED CT) free to use in India and appointing an interim National Release Centre to handle the clinical terminology standard, which is gaining widespread acceptance among healthcare IT stakeholder communities worldwide. In addition, the MoHFW has proposed a new bill, the DISHA, to regulate data security in the healthcare industry. This Act's goal will be to protect the privacy, confidentiality, security, and standardisation of electronic health data. Through the proposed DISHA, the MoHFW intends to establish a statutory body to promote and adopt e-health standards, enforce privacy and security measures for electronic health data, and regulate the storage and interchange of EHR. To meet the standards, the Personal Data Protection Bill, 2019 was introduced in Lok Sabha on December 11th, 2019, with the goal of protecting people's personal data and establishing a Data Protection Authority.

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

Hospitals, research organisations, and technological service providers are among the entities participating in data gathering, record-keeping, and information exchange. These procedures can also be updated in response to ongoing experiences and issues encountered during the transition, lag phase, and connecting the consumer and service provider.

4.3 Which key regulatory requirements apply?

The MoHFW intends to create a statutory body in the form of a national digital health authority to promote and adopt e-health standards, enforce privacy and security measures for electronic health data, and regulate the storage and exchange of EHR through the proposed DISHA. In addition, the National Digital Health Authority (NeHA) under the Ministry of Health and Family Welfare is a proposed authority that will oversee developing an integrated health information system in India. It is proposed that it serve as a promotional, regulatory, and standard-setting body to guide and support India's digital health journey and the subsequent realisation of the benefits of ICT intervention in the health sector. It also explains NeHA's intended functions and governance structure. DISHA is a piece of legislation that aims to formally establish NeHA and promote the online exchange of patient data to avoid duplication of efforts and resources.

4.4 Do the regulations define the scope of data use?

Yes, the regulations identify the scope of information use with beneficiary and service provider permission, as well as the criteria for "sensitive health-related information" and "sensitive personal information".

4.5 What are the key contractual considerations?

The primary contractual consideration to ensure secrecy and privacy for the various phases of the investigation, from data collection to data use, would be to enter into non-disclosure and personal privacy agreements with employees and other influencers participating in the research, as well as to offer additional solutions for breaches of pre-defined contractual conditions.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Purposeful sampling and data confidentiality are major concerns, and there are challenges due to the lack of defined legal remedies. This is a critical need and requirement to safeguard and secure full rights to increase the probability and expectation of improving care and a more excellent healthcare system based on evidence.

5 Data Sharing

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

Some of the key issues to consider when sharing personal data include: flexibility and those associated with data collection and transfer; security and privacy during the transformation process; and information sharing, trust, responsibility, and accountability.

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

Such considerations are essential and largely dependent on the overall number of subjects and scientific entities participating. Furthermore, the aim of using data protection and privacy to achieve quick results might influence data sharing, which is an important factor that should be checked at every step of the process by all parties involved.

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

The MoHFW developed the DISHA proposal with the goal of protecting healthcare data in India and giving consumers complete control over their health data. For example, if a patient visits the doctor for a check-up and the doctor looks up the patient's previous medical history and enters the current diagnostic results into an EHR, DISHA ensures that the information is completely secure as it moves through the healthcare system. DISHA outlines three key goals for data protection: establishing a national and state-level digital health authority, enforcing privacy and security measures for electronic health data, and regulating electronic health information storage and interchange. Furthermore, the proposal calls for the establishment of National and State Electronic Health Authorities (NeHA and SeHA) to provide comprehensive data protection and healthcare management for Indian citizens, as well as to ensure and monitor data portability.

6 Intellectual Property

6.1 What is the scope of patent protection?

India has been adopting and implementing the terms of the Patents Act, 1970, which offers patent protection and is consistent with Trade-Related Aspects of Intellectual Property Rights (TRIPS). To get patent protection in India, the invention

must not come within the scope of Sections 3 and 4 of the Act, in addition to meeting the patentability requirements of novelty, inventive step, and industrial applicability. Section 3(k) of the Indian Patents Act, which prohibits the patentability of a computer program in and of itself, is relevant because any digital health application relies on software and a computer program. Furthermore, the Delhi High Court clarified that not all computer programs are exempt from Section 3(k), and that the invention is patentable if the program exhibits a "technical effect" or a "technical contribution".

Furthermore, under Section 3(i) of the Indian Patents Act, a patent may not be granted if the program or method is directed to "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". The apparatus and method of using an *in vitro* mechanism, on the other hand, are patentable.

6.2 What is the scope of copyright protection?

In India, the Copyright Act of 1957 protects copyright. Original literary, dramatic, musical, or aesthetic work, cinematograph films, and sound recordings can all be protected by a copyright. Although copyright registration is not required, it does serve as *prima facie* proof in establishing the legal claim. Because digital health applications are fundamentally software, they will fall under the definition of a "computer program" and be protected under Indian copyright laws.

6.3 What is the scope of trade secret protection?

In India, there is no specific law governing the handling of confidential information and trade secrets. In the emerging digital health industry, however, such sensitive information is normally safeguarded by mutual agreements such as non-disclosure and confidentiality agreements.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

In India, the concept of academic technology transfer is still in its infancy. Though universities and some companies have embraced this concept and developed rules for strategically deploying innovations as well as rewarding inventors. Furthermore, protecting intellectual property in the digital health sector is still in its initial phases, but it is increasing exponentially, and academic and research organisations are increasingly aware of the importance of protecting and disseminating their knowledge through technology transfer, and the trend appears to be continuing with better results. Typical academic technology transfer rules and activities include, but are not limited to, the following steps: evaluation/assessment of the proposed invention in terms of patentability and commercialisation; intellectual property protection in various domains relating to the concerned technology; and searching and identifying the most suitable partner for licensing and monetising the proposed technology and invention's working.

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

The Indian Patents Act, Section 3 (k), prohibits the patentability of computer programs in general. The Delhi High Court has clarified that Section 3(k) does not apply to all computer programs, and that such programs are patentable if they establish a "technical effect" or "technical contribution". Furthermore, a patent may not be granted under Section 3(i) of the Indian Patents Act if the program or process is directed to "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". The apparatus and method of using an *in vitro* mechanism are patentable.

As digital health applications are fundamentally software, they should be classified as "computer programs" and protected under Indian copyright laws. In addition, class 9, which includes computer software and computer programs, is one of the classes in which a trademark can be registered.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

No, an artificial intelligence device cannot be named as an inventor of a patent in India.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

As of now, there are no specific rules for government-funded innovations.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

To ensure effective collaborative improvements, various considerations not limited to the following can be practically applied for collaborative improvements, such as: primary objectives for collaborating; details of all eligible members and parties involved; consideration of management of governance along with dissemination of contract management; confidentiality and evaluation of existing intellectual property and technology transfer procedures; and information regarding allocating payments, rights, obligations, liabilities, variations, termination and other related factors are important facts for consideration while applying for collaborative improvements.

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

In terms of internal communications and offering services externally, the working concepts and work-flow procedures for healthcare and non-healthcare organisations are completely different; nonetheless, client happiness is the primary priority for both sectors. Apart from the confidentiality protocol for data exchange, data protection, security and privacy, approaches to sharing information must also be examined when evaluating agreements.

8 AI and Machine Learning

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

The key responsibilities of machine learning in digital health include: ease of using numerous methods and processes to decrease cost, time, and effort; identification and early detection of disease; assistance with drug development and production; examining behaviour modifications based on machine learning; to keep and secure medical records; outbreak prediction; and clinical experiment, data collecting, and interpretation.

8.2 How is training data licensed?

There are currently no unique rules controlling AI, cloud computing, or machine learning in India, therefore activities employing these technologies must follow standard IT laws and regulations. A confidentiality agreement between the licensee and the licensor, as well as the intended use of the captured data, would be advantageous.

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 presently not applicable in India. Furthermore, in India, algorithms are not patentable subject matter.

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

Authenticity of licensed data, permission for various users and beneficiaries, consideration for purposes such as "know-your-customer", restriction and limited access on multiple locations and multiple users, data privacy and security, quality, rights for using, term and termination are all important factors to consider.

9 Liability

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

Liabilities for negative consequences might be civil or criminal, and they differ between practitioners who give services and service providers such as institutes and internet vendors. Civil proceedings, for example, can make use of the Consumer Protection Act's remedies in addition to filing a civil complaint. In the event of a doctor's negligence, a customer can also file a complaint with the Medical Council of India's ethical committee. Furthermore, the Indian Penal Code covers criminal liability, which would also apply to digital health solutions.

9.2 What cross-border considerations are there?

The use of data applications and data localisation is of the utmost importance.

10 General

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

The high expense of establishing and maintaining health information technology, as well as keeping data while protecting secrecy and privacy, is a constant concern in digital health. Another key issue that requires consideration is the security and privacy of data management in various stages of transformation.

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

Non-healthcare enterprises must recognise that the health sector follows highly regulated manufacturing and marketing requirements, in addition to competent business planning and data privacy and security approaches. In addition, consumer protection rules apply to the healthcare industry.

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

A proper business plan, market opportunities, strategic partnerships, understanding of financial and key matrices for business, potential risk for business, expected valuation, regulatory compliances, and IP protection are some of the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Interoperability of data – particularly health records – data security and privacy are the main impediments to mainstream clinical use of digital health technologies.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

There are currently no such certifying bodies.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

As of now, there are no explicit standards governing reimbursement or any formal accreditation of solution providers.

Manisha Singh is the founder and the managing partner of LexOrbis. She oversees and supervises all practice groups at the firm. Manisha is known and respected for her deep expertise in the prosecution and enforcement of all forms of IP rights and for strategising and managing the global patents, trademarks, and design portfolios of large multinationals and domestic companies. She is also known for her sharp litigation and negotiation skills for both IP and non-IP litigations and dispute resolution. She has represented companies in many IP litigations with a focus on patent litigation covering all technical fields, but particularly pharmaceuticals, telecommunications, and mechanics.

LexOrbis
709–710 Tolstoy House, 15–17 Tolstoy Marg
New Delhi-110001
India

Tel: +91 11 2371 6565
Email: manisha@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, as well as a patent agent. He has a Master's degree in pharmaceutical science and management. He regularly advises clients on IP strategy and portfolio management. Pankaj has in-depth knowledge of patent law and the healthcare regulatory framework in India, as well as extensive experience in patent filing, drafting, prosecution, and advisory matters, especially in the chemical, pharmaceutical, and start-up fields. He has written several articles and delivered talks at various forums on patent law practice, the 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 one of the fastest growing intellectual property firms in India, with offices in three strategic locations: Delhi; Mumbai; and Bengaluru. With a team of over 90 highly reputed lawyers, engineers, and scientists, the firm acts as a one-stop shop and provides practical solutions and services for all IP and legal issues faced by technology companies, research institutions, universities, broadcasters, content developers, and brand owners. Its services include Indian and global IP portfolio development and management (patents, designs, trademarks, copyright, GUI, plant varieties, etc.), advisory and documentation services on IP transactions/technology-content transfers, and IP enforcement and dispute resolution before all forums across India. The firm has a global reach with trusted partners and associate firms.

www.lexorbis.com

Ireland


Colin Kavanagh


Colin Rooney


Bridget McGrath


Caoimhe Stafford

Arthur Cox LLP

1 Digital Health

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

There is no definition of "digital health" in Irish legislation. Digital health is generally accepted as referring to standalone software, health technologies and apps used in the healthcare sector, or those used in combination with other products.

1.2 What are the key emerging digital health technologies in your jurisdiction?

Some of the key emerging technologies are as follows:

1. **Telemedicine** – the delivery of healthcare by registered healthcare practitioners to patients using online platforms or health apps.
2. **Artificial Intelligence (AI)** – the use of advanced computer technologies, predictive analysis and machine learning is ever-increasing in the life sciences and healthcare sectors.
3. **Health Apps** – apps hosted on connected wearables and mobile devices which aim to monitor and improve health/wellbeing.

1.3 What are the core legal issues in digital health for your jurisdiction?

Some of the core legal issues in healthcare are as follows:

1. **Product Classification** – the convergence of medical devices, medicinal products and software requires that product classification is carefully considered to ensure regulatory compliance.
2. **Data Protection and Cybersecurity** – patient data must be collected and handled in compliance with data protection law.
3. **Product Safety** – in order to ensure patient safety, all products must comply with applicable product safety legislation.

1.4 What is the digital health market size for your jurisdiction?

Although this is difficult to quantify in the Irish context, based on Ireland's significant presence in the life sciences, technology and social media sectors, the ever-evolving digital health market in Ireland is on track to hold a significant share of the estimated $100 billion global digital health market.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

This information is not currently available.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

1. **Healthcare Framework**
   The Health Act 1970 (as amended) sets out the statutory basis for the structure of the national healthcare system. The Department of Health determines healthcare policy and expenditure. This is implemented by the national health provider, the Health Service Executive (HSE). The Health Information and Quality Authority (HIQA) is a statutory body responsible for regulating and accrediting public hospitals, implementing quality assurance programmes, and evaluating the clinical and cost effectiveness of health technologies.
2. **Healthcare Professionals**
   Healthcare professionals are regulated as follows:
   - The Medical Practitioners Act 2007 – registered medical practitioners.
   - The Nurses and Midwives Act 2011 – nurses and midwives.
   - The Pharmacy Act 2007 – pharmacists and pharmaceutical assistants.
   - The Health and Social Care Professionals Act 2005 – includes, amongst others, occupational therapists, speech and language therapists and social workers.
3. **Medical Devices**
   Directive 93/42/EEC concerning medical devices and Directive 90/385/EEC on active implantable medical devices were entirely replaced by Regulation (EU) 2017/745 on medical devices (MDR) on 26 May 2021, however, certain transitional provisions apply to certain devices (Medical Device Legislation).
   The Health Products Regulatory Authority (HPRA) is the Competent Authority responsible for regulating medical devices. The National Standards Authority of Ireland (NSAI) is the Notified Body designated by the HPRA to carry out conformity assessment procedures to ensure compliance with Medical Device Legislation.
4. **Medicinal Products**
   The regulatory framework for pharmaceuticals is based on Directive 2001/83/EC on the Community code relating

to medicinal products for human use (as amended). This was implemented by the Irish Medicines Board Act 1995 (as amended) and domestic regulations. The HPRA is the medicines regulator.

5. **Telemedicine**
   There is no legislation specifically regulating telemedicine in Ireland. However, the current Medical Council Guide to Professional Conduct and Ethics for Registered Medical Practitioners states that telemedicine services can be provided, subject to:
   - strong security measures;
   - patients providing their consent to:
     - the consultation being conducted through telemedicine;
     - any treatment provided;
   - information policies being clear to users;
   - services being safe and suitable for patients;
   - the patient's general practitioner being informed of the consultation; and
   - intra-jurisdictional transfers of personal patient information complying with data protection principles.

Further, healthcare providers of telemedicine services to patients within Ireland must be registered with the Medical Council. Derogations from the Medical Council Guide may constitute a breach of professional duty by medical doctors.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

If digital health products are classified as medical devices, the Medical Device Legislation will apply.

Directive No. 2001/95/EC on general product safety, as amended (GPSD), which is transposed into Irish law by the European Communities (General Product Safety) Regulations 2004, may apply to digital health and healthcare IT products which do not fall within the scope of Medical Device Legislation. The Consumer Protection Act 2007, which gives effect to Directive No. 2005/29/EC on unfair commercial practices, may also apply to digital health consumer products.

The Liability for Defective Products Act 1991 (LDPA) implements Directive No. 85/374/EEC on liability for defective products into Irish law.

The use of personal data in digital health technologies and healthcare IT is primarily regulated by the General Data Protection Regulation (GDPR) and the Data Protection Acts 1988–2018.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Generally speaking, the following regulatory schemes apply to consumer healthcare devices or software:

- Medical Device Legislation (where the product is a medical device).
- Product Safety.
- Product Liability.
- Consumer Protection.
- Data Protection.
- Cybersecurity.
- Intellectual Property (IP).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

HIQA is a statutory body responsible for regulating and accrediting public hospitals, implementing quality assurance programmes, and evaluating the clinical and cost effectiveness of health technologies.

The HPRA is the Competent Authority for the regulation of health products, including medicines, medical devices and cosmetics.

The Competition and Consumer Protection Commission (CCPC) is the statutory body responsible for enforcing consumer protection and general product safety legislation.

The Data Protection Commission (DPC) is the Irish supervisory authority for the purposes of the GDPR.

The NSAI is Ireland's official standards body that creates, maintains, promotes and issues accredited certification of products, services and organisations with recognised standards.

The Department of Health is the government department tasked with the delivery of policies for the health sector.

The Medical Council is the regulatory body of medical doctors in Ireland and maintains the Register of Medical Practitioners.

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

The delivery of digital health. All registered medical practitioners must be appropriately registered with the Medical Council of Ireland and operating in compliance with applicable legislation and ethical standards.

Patient safety is of paramount importance in the delivery of appropriate healthcare. Accordingly, product safety and liability are key enforcement areas for the HPRA and CCPC.

Privacy and security are also key enforcement areas in terms of healthcare IT. The DPC has wide-ranging powers, and can impose substantial sanctions for breaches of the GDPR. Further, data subjects have the right to bring actions for material and non-material damages in the courts.

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

Software as a medical device is regulated by the Medical Device Legislation. Approval for clinical use is assessed by either the device manufacturer (the device is subject to the self-certification conformity procedure) or a Notified Body.

2.7 What regulations apply to Artificial Intelligence/Machine Learning powered digital health devices or software solutions and their approval for clinical use?

Depending on the specific product and its function, the legislation referred to above will apply. Approval for clinical use will be assessed by the manufacturer if subject to the 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?

- **Telemedicine/Virtual Care**
  As there is no specific legislation regulating telemedicine in Ireland, healthcare providers and companies offering telemedicine services must comply with a range of related and applicable legislation, regulation and guidance. Core issues include compliance with prescribing regulations and the applicability of the medical devices framework.
- **Robotics**
  Product liability and allocation of liability are key issues relating to the use of robotics in the life sciences and healthcare sectors. IP issues may also arise.
- **Wearables**
  The applicability of Medical Device Legislation to wearables is a core issue. Product safety, product liability, consumer protection and data protection are also pressing concerns regarding the use of wearables.
- **Virtual Assistants (e.g. Alexa)**
  Cybersecurity and data protection concerns are core issues relating to the use of virtual assistants. Liability and product safety issues may also arise regarding the use of virtual assistants and particularly as regards their interaction with connected devices.
- **Mobile Apps**
  See Telemedicine and Wearables.
- **Software as a Medical Device**
  When software is classified as a medical device, core issues relating to the use of that software, aside from compliance with Medical Device Legislation, include cybersecurity, data protection and consumer protection.
- **Clinical Decision Support Software**
  See Software as a Medical Device.
- **AI/ML powered digital health solutions**
  See Software as a Medical Device. Cybersecurity and data protection are also key issues, as are product safety, liability and consumer protection.
- **IoT and Connected Devices**
  Cybersecurity is of paramount importance regarding Internet of Things (IoT) and connected devices, particularly regarding unauthorised access attempts. Data protection, product liability and consumer protection are also important.
- **3D Printing/Bioprinting**
  3D-printed products may be used to produce medical devices which fall within the scope of Medical Device Legislation. Accordingly, compliance with Medical Device Legislation and applicable conformity assessment and CE-marking procedures will be a core issue. Product liability and IP concerns may also arise.
- **Digital Therapeutics**
  This will depend on the specific nature of the product. See core issues that apply to all of the above.
- **Natural Language Processing**
  Natural Language Processing may give rise to concerns around data protection, product safety, liability and IP.

3.2 What are the key issues for digital platform providers?

Where there is no specific regulatory regime for digital health in Ireland, digital platform providers must comply with a range of related and applicable legislation, regulation and guidance.

Data protection and, particularly the use, storage and transfer of personal data are key issues for digital platform providers, as is cybersecurity. In particular, digital platform providers must adopt measures to protect against and prevent the occurrence of malware virus attacks, particularly where large amounts of sensitive personal data are stored within their platforms.

4 Data Use

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

In conducting any activities that involve the processing of personal data, companies must adhere to the key principles in Article 5 GDPR. These can be summarised as follows:

- **Lawfulness, Fairness and Transparency**: All processing activities must have a legal basis under Article 6 GDPR, meaning the processing must be: (a) based on data subject consent; (b) necessary to perform a contract with the data subject; (c) necessary to comply with a legal obligation; (d) necessary to protect a person's vital interests; (e) necessary to perform a task in the public interest; or (f) necessary to achieve the legitimate interests of the controller or a third party, where those interests outweigh the rights and freedoms of the relevant data subject(s). Where special categories of data are concerned (including health data, genetic data and biometric data), controllers must identify an exemption under Article 9 GDPR (e.g. explicit consent). Reliance on such exemptions may be subject to further conditions under the Data Protection Acts 1988–2018. Controllers must also facilitate data subjects in the exercise of their rights under Articles 15–22 GDPR, and ensure any transfers of personal data outside the European Economic Area (EEA) are made subject to the adoption of appropriate measures. To ensure transparency, data subjects must receive user-friendly information about how their personal data is processed, including but not limited to all information in Article 13/14 GDPR.
- **Purpose Limitation**: Personal data must only be processed for the specific purposes communicated to the data subject, and cannot be processed in a manner incompatible with those purposes.
- **Data Minimisation**: No more personal data than is needed for the controller's purposes should be collected, and it should not be shared more widely than is necessary.
- **Accuracy**: Personal data must be accurate and kept up-to-date. Inaccurate data must be promptly rectified or erased.
- **Storage Limitation**: Save for limited exemptions (e.g. for scientific research and statistical purposes), personal data should be deleted or anonymised when it is no longer necessary.
- **Integrity and Confidentiality**: Controllers must implement appropriate technical measures and policies to ensure personal data is processed securely, and to protect against unauthorised or unlawful processing or accidental loss, destruction or damage (i.e. a data breach).
- **Accountability**: Controllers are responsible for demonstrating compliance with their obligations under the GDPR. Where any digital health offering involves the processing of health data and could potentially pose high risks to data subjects, a data protection impact assessment must be conducted in advance of the processing. Such assessments and records of processing help controllers to

demonstrate accountability. If a company's core activities involve the processing of special categories of personal data, they will also need to appoint a data protection officer.

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

Whether the entity is public or private will impact on the legal bases that can be relied upon (e.g. public bodies cannot rely on their legitimate interests (Article 6(1)(f) GDPR) to conduct official activities). Public bodies are also subject to the Data Sharing and Governance Act 2019.

Controllers bear primary responsibility for compliance with data protection law, insofar as they decide how and why personal data is processed. Where they engage vendors/service providers to process personal data on their behalf, they must vet them in advance, and enter data processing agreements with robust safeguards, as explained in question 4.5.

4.3 Which key regulatory requirements apply?

The GDPR, as supplemented by the Data Protection Acts 1988–2018, contains the core data protection rules.

To the extent digital health technologies may involve the use of cookies, or where organisations want to market to individuals, the ePrivacy Directive 2002/58/EC (as amended) and the Irish ePrivacy Regulations are also relevant.

Where health data is collected for the purpose of health research, the Data Protection Act 2018 (Section 36(2) (Health Research) Regulations 2019 (as amended) (Health Research Regulations) will apply, and the controller will be subject to extensive obligations, including the need to obtain the explicit consent of data subjects. If it is not possible/appropriate to obtain the explicit consent of data subjects, controllers may apply to the Health Research Consent Declaration Committee for a declaration that the explicit consent of data subjects is not required where the public interest in conducting the health research "*significantly outweighs*" the public interest in obtaining their explicit consent.

The Data Protection (Access Modification) (Health) Regulations 1989 put parameters around access to health information, recognising the important role of health professionals regarding this data.

The Data Sharing and Governance Act 2019 introduced additional statutory obligations for public bodies.

4.4 Do the regulations define the scope of data use?

Although the GDPR is a principle-based regulation, meaning it is not highly prescriptive as to how data can be used, it places clear obligations on controllers to respect data subjects' information. The Irish legislation outlined above is more explicit regarding how organisations can use data.

4.5 What are the key contractual considerations?

Where a controller appoints a data processor to process personal data on its behalf, both parties must enter a written data processing agreement (DPA) that meets the requirements of Article 28 GDPR.

Where two or more parties are working together, they may be considered "joint controllers" if they are jointly deciding the purposes and means of processing personal data. In such circumstances, joint controllers would be well advised to enter a written contract setting out the respective responsibilities of each party, as joint controllership implies joint liability for breaches of data protection law, and the "essence" of the arrangement must be further communicated to data subjects.

It is worth including detailed data protection provisions in any contract concerning the disclosure of personal data.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Where data is exchanged pursuant to a contract, ownership of that data (and rights regarding its use) should be set out very clearly.

Where personal data is concerned, the parties to any digital health offering must be aware of their roles and responsibilities, and controllers must have valid legal grounds for the collection and use of the personal data.

Data subjects cannot waive their rights of access, rectification, erasure, restriction, objection and portability, and the right to not be subject to automated decision-making. As such, controllers must be in a position to promptly and effectively facilitate the exercise of data subject rights.

5 Data Sharing

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

As noted in our answer to question 4.1, the GDPR restricts the transfer of personal data outside the EEA. This has significance where controllers wish to share personal data with partners/service providers in "third countries".

Personal data can be freely transferred to countries which have received an "adequacy decision" from the European Commission. Otherwise, certain safeguards must be implemented (e.g. data exporters and data importers may execute the European Commission-approved Standard Contractual Clauses). Following the recent decision of the Court of Justice of the European Union in case C-311/18 (Schrems II) and subsequent regulatory guidance, data exporters must also verify on a case-by-case basis that the personal data being transferred will be afforded an "essentially equivalent" level of protection in the destination country, and adopt technical, contractual and/or organisational measures as appropriate to mitigate risks.

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

The Data Sharing and Governance Act 2019 regulates the ability of public bodies (including the HSE) to share personal data with other public bodies. The majority of its provisions do not apply to special categories of personal data, which may limit its applicability to data sharing in a healthcare context.

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

Any transfers of personal data outside the EEA must comply with Chapter V GDPR, and the Data Sharing and Governance Act 2019 regulates the sharing of data by public sector bodies. As outlined in our answer to question 4.5, appropriate contractual arrangements should be entered into where personal data is shared between parties.

6 Intellectual Property

6.1 What is the scope of patent protection?

The Patents Act 1992 (as amended) governs the law relating to patents. For an invention to be patentable, it must be susceptible of industrial application, new and involve an inventive step.

To register a patent in Ireland, applicants must file at the Intellectual Property Office of Ireland or at the European Patent Office with an Irish designation.

Full-term patents can provide protections for up to 20 years. A short-term patent may be obtained without needing to demonstrate the invention's novelty.

A patent cannot be obtained for, among other things:

- a discovery, scientific theory or mathematical method;
- a scheme, rule or method for performing a mental act, or a computer program;
- the presentation of information; or
- 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 (excluding a product, substance or composition for use in any such method).

6.2 What is the scope of copyright protection?

The Copyright and Related Rights Act 2000 (as amended) (2000 Act) governs the law relating to copyright. It was recently amended by the Copyright and Other Intellectual Property Law Provisions Act 2019, which also provided more recourse to rights in the Irish courts.

Copyright subsists automatically upon the creation of literary, artistic and other tangible works (including computer programs) and databases, protecting the physical manifestation of the work (as distinct from the underlying idea or principle) once the work in question meets the test of originality under copyright law.

In an employment context, the employer will be the first owner of any copyright created by an employee in the course of their employment, unless they have agreed otherwise.

The owner of copyright in a work has the exclusive right to prevent or allow others to:

- copy the work;
- perform the work;
- publish or otherwise make available the work; and
- adapt the work.

6.3 What is the scope of trade secret protection?

The protection of trade secrets is governed by the European Union (Protection of Trade Secrets) Regulations 2018 (Trade Secrets Regulations), which transpose Directive EU 2016/943 (the Trade Secrets Directive) into Irish law. Under this regime, a trade secret is protected if:

- it is secret, being not generally known among or readily accessible to persons who normally deal with that kind of information;
- it has commercial value because it is secret; or
- reasonable steps have been taken to keep it secret.

The Trade Secrets Regulations provide for prohibitive and corrective remedies in order to prevent and/or obtain redress for the unlawful acquisition, use or disclosure of the trade secret.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

Knowledge Transfer Ireland is the national office tasked with facilitating the transfer of academic and state-funded expertise and technology to businesses. They produce model agreements which typically form the basis for the licensing of university-generated IP to spin-out companies or industry investors in return for royalties and for collaborative developments between industry and academia.

IP owned or developed by academic institutions may also be assigned provided 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?

Copyright in the software itself (source and object code) is protected by copyright. Any accompanying elements such as sound and graphic designs are also protected by copyright.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

Although there is no case law on this question in Ireland, the legislation envisages that the inventor will be a natural person, with section 17 of the Patents Act 1992 requiring patent applicants to identify the "person or persons whom he believes to be the inventor or inventor", and the Patent Rules requiring the applicant to provide their address. This is supported by a recent decision of the UK Court of Appeal (*Thaler v Comptroller General of Patents Trade Marks and Designs [2021] EWCA Civ 1374*) where the Court held that an artificial intelligence machine cannot qualify as an "inventor" for the purposes of the UK Patents Act 1977 because it is not a person within the meaning of the legislation.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

Government grants are often awarded subject to a range of conditions relating to intellectual property, in respect of which compliance is required.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Parties should contractually agree the manner in which the resulting IP (including any improvements to pre-existing IP) will be owned and licensed as well as matters of confidentiality and commercialisation.

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

Healthcare companies are subject to specific regulatory and reporting obligations in respect of their activities which will need to be recognised and reflected in the agreement governing its activities with any other company. Depending on the nature

and extent of the activities being conducted by each party, particular consideration should be given to issues of reporting, quality standards, confidentiality and protection over proprietary IP and liability and claims management.

Where a contract relates to a product, as defined by the Product Liability Directive, then a strict liability regime will apply to each of the developers, manufacturers and potentially the suppliers and distributors depending on the necessary facts. The ability for a party to limit its liability in a contract is also impacted by consumer law.

8 AI and Machine Learning

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

Machine learning continues to play an increasingly important role in digital health, particularly regarding diagnostics, patient monitoring and decision support systems. Of course, the use of AI should enhance and not replace the role of the healthcare practitioner.

8.2 How is training data licensed?

Training data can be licensed in the same way as any other proprietary data or technology (governing issues such as field of use, warranties and disclaimers, and confidentiality). Please see our response to question 8.4 below.

Under the Open Data Strategy 2017–2022, the Irish Government licenses open (non-personal) data sourced from the activities of public bodies using the Creative Commons (CC-BY) Licence. This licence allows others to distribute, adapt and build upon data for commercial or non-commercial purposes, provided the originator is credited for the original creation.

Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market (as recently implemented in Ireland by the European Union (Copyright and Related Rights in the Digital Single Market) Regulations 2021) provides research organisations with a mandatory exception to copyright that allows them to extract and reproduce text and data from databases or other sources to which they have lawful access in order to carry out data mining for the purposes of scientific research. A more restrictive regime applies to commercial text and data mining.

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 the 2000 Act, the author of a work generated by a computer in circumstances where the author of the work is not an individual is the person who made the arrangements necessary for the creation of the work. Although there is no Irish case law on this point as yet, it is likely that the engineers who assemble the models and software which improve the algorithm would individually and collectively be considered the "authors", and would therefore own the IP in the improved algorithms. As noted in our answer to question 6.2, copyright would vest in their employers if they generated the copyright in the course of their employment unless there was an agreement to the contrary.

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

The parties should consider the strength of any warranties as to the completeness, accuracy and usefulness of the licensed data, data protection compliance, the ownership of background IP and IP that is generated by using the data, and the scope of the licence.

9 Liability

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

Liability for adverse outcomes in digital health can arise under:

- Contract: Liability can arise under the Sale of Goods Act 1893, as amended by the Sale of Goods and Supply of Services Act 1980.
- Tort: The general common law principle of duty of care applies. Therefore, product manufacturers owe a duty of care to all those who may be foreseeably injured or damaged by their products.
- Statutory Liability: The LDPA implements Directive 85/374/EEC on liability for defective products (Product Liability Directive) into Irish law.
- Criminal: The European Communities (General Product Safety) Regulations 2004 implement the provisions of the GPSD.
- Medical Devices: Digital health products that are classified as medical devices will be subject to liability arising under Medical Device Legislation.
- Clinical Negligence: Liability in the context of clinical negligence may arise where a medical practitioner breaches a duty of care owed to a patient and damage or injury is suffered by the patient as a result.

9.2 What cross-border considerations are there?

Under the Rome I Regulation and the Rome II Regulation, Irish law will apply to contractual and non-contractual (e.g. personal injury) claims arising in relation to digital health delivery to patients, irrespective of the country of origin of the digital health provider.

10 General

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

Compliance with data protection law is critical where a service entails the sharing of special categories of personal data, particularly outside the EEA. Strong measures must be adopted to maintain the security of the services and mitigate against the risks of a data breach.

Cloud-based service providers in the digital health space should also consider if they fall within the scope of the EU Directive on the Security of Network and Information Systems (NIS Directive), as transposed into Irish law by the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 and the Commission Implementing Regulation (EU) 2018/151. The

legislation imposes a range of cyber-security rules on operators of essential services (OES) and digital service providers (DSPs). Non-computing cloud solutions do not fall within the definition of DSPs. Service providers may be an OES in limited circumstances – where they fall within a category of activity (including the "health sector"), they fulfil various criteria and they are designated by the competent authority.

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

Non-healthcare companies should adopt a holistic approach when navigating the relevant legal and regulatory requirements at an early stage of development of services and related technology. As the regulation and guidance around telemedicine is developing rapidly, companies should maintain a dialogue with the relevant regulatory authorities to confirm whether the authorities are drafting or preparing any guidance that might be relevant.

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

Prior to investing in digital healthcare ventures, venture capital and private equity, firms should consider whether:

- appropriate procedures are in place for regulatory compliance;
- the target companies own all of the necessary IP and have patent protection in place; and
- appropriate supply and service contracts are in place.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Some of the key barriers holding back widespread clinical adoption of digital health solutions are as follows:

- Fewer clinical trials in the area of digital health solutions are conducted, which in turn results in lower rates of demonstrated clinical and economic benefit or safety and efficacy.
- Lack of a harmonised approach and overarching legislation across the EU.
- Cybersecurity and privacy concerns.
- Product safety and liability allocation concerns.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The Medical Council regulates medical doctors in Ireland and provides input on policy and legislation in this area, as well as guidance on professional conduct and ethics in this area. The Pharmaceutical Society of Ireland carries out a similar role for pharmacists in Ireland and would be active in this area. There are a number of industry bodies relevant to the digital health sector under the auspices of IBEC (Irish Business and Employers Confederation), including the Irish MedTech Association, BioPharamChem Ireland and Technology Ireland, driving policy initiatives and cross-sectoral strategies relevant to the digital health sector. eHealth Ireland, a HSE initiative, assists in the delivery of improved digital health across Ireland.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

This will depend on the specific product. In order to receive reimbursement approval under one of the State schemes in Ireland, a product supplier must apply to the HSE for inclusion on the HSE's reimbursement list. Where products are not available for reimbursement under a State reimbursement scheme, a patient may pay privately for a product or service. Private health insurers may reimburse patients for access to certain products or services, depending on the level of cover of the insured.

Colin Kavanagh is a partner in the Corporate and M&A Department and Head of the Life Sciences Group. Colin advises Irish and multi-national pharmaceutical, medical device, digital health, biotech, cosmetic, food, beverage and agri-business companies in Ireland on a wide range of corporate M&A, commercial, regulatory, intellectual property and promotional matters.

Arthur Cox LLP
Ten Earlsfort Terrace
Dublin 2, D02 T380
Ireland

Tel: +353 1 920 1196
Email: colin.kavanagh@arthurcox.com
URL: www.arthurcox.com

Colin Rooney is a partner in the Technology and Innovation Group. His practice focuses on technology matters, with a particular focus on data privacy and data security and covers a broad range of work, ranging from regulatory dealings and negotiations, to compliance and counselling agreements. Colin also advises on digital transformation, online trading matters, and has extensive experience advising on commercial IT agreements.

Arthur Cox LLP
Ten Earlsfort Terrace
Dublin 2, D02 T380
Ireland

Tel: +353 1 920 1194
Email: colin.rooney@arthurcox.com
URL: www.arthurcox.com

Bridget McGrath is an associate in the firm's Regulated Markets Group with specialist expertise in life sciences regulation. Bridget advises clients in the pharmaceutical, biotech, digital health and medical device sectors in relation to the entire product lifecycle, including clinical research and market access, promotional and compliance issues, pricing and reimbursement and transactional matters.

Arthur Cox LLP
Ten Earlsfort Terrace
Dublin 2, D02 T380
Ireland

Tel: +353 1 920 1298
Email: bridget.mccgrath@arthurcox.com
URL: www.arthurcox.com

Caoimhe Stafford is an associate in the Technology and Innovation Group. Caoimhe's main areas of practice are data protection, commercial contracts, e-commerce, freedom of information, gambling and betting and intellectual property. She is a member of our Dawn Raid Response Unit, and regularly advises international and domestic clients on complex privacy queries in respect of cross-border processing and novel technologies. She frequently collaborates with the Employment Group to advise on data protection compliance in the context of employment disputes and human resources management.

Arthur Cox LLP
Ten Earlsfort Terrace
Dublin 2, D02 T380
Ireland

Tel: +353 1 920 1328
Email: caoimhe.stafford@arthurcox.com
URL: www.arthurcox.com

Our digital health Group is recognised as market leader in Ireland, combining subject-matter experience, in-depth industry knowledge and strategic problem-solving to advise our clients in relation to novel legal and regulatory issues in this rapidly evolving sector.

Our clients include multinational and start-up pharmaceutical companies, medtech and biotech manufacturers, healthcare organisations, research institutions and telemedicine providers.

Relevant Experience:

- Advising a global tech company in relation to the regulation of its telemedicine platform.
- Advising a leading European telemedicine provider in relation to the regulation of its platform and proposed establishment of Irish operations.
- Advising a global administrative service provider for the healthcare industry in relation to the regulation of digital technologies, and its operations and interactions with healthcare professionals and regulators.
- Advising a leading European telemedicine platform on proposed operations in Ireland, including interactions with healthcare professionals, pharmacies and the regulation of e-prescriptions.
- Advising a leading pharmaceutical wholesaler in relation to the regulation of prescriptions and courier delivery of medicinal products
- Advising a global medical device manufacturer in relation to the delivery of telemedicine services.
- Advising a global financial services and insurance provider in relation to the regulatory aspects of a proposed telemedicine project.

www.arthurcox.com

ARTHUR COX

Israel


Eran Bareket


Alexandra Cohen

Gilat, Bareket & Co., Reinhold Cohn Group

1 Digital Health

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 digital health technologies in your jurisdiction?

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 digital health for your jurisdiction?

The core legal issues in digital health in Israel 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 start-ups.
- 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:

- Regulation for the use of health data (goals, manner of use, users, transparency).
- Regulation for the use of remote medical care (the manner in which the service is provided and service provider obligations).
- Regulation for the access of personal electronic health record files by patients.
- Regulation for determining the minimum content of the electronic health records.
- Regulation applying on outcome measures of health data, which collect and monitor health data.
- Regulation for the development and maintenance processes of clinical information systems.
- Regulation for aspects of cyber protection of data.

1.4 What is the digital health market size for your jurisdiction?

According to the Start-Up Nation Central's report, Israeli digital health companies raised more than $1 billion in the first half of 2021. There is no publicly available data regarding market size in terms of revenues.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

Private companies are not required to publish their financial results, therefore there is no detailed information regarding the revenue of private digital health companies in Israel. However, among the companies that raised significant amounts in 2021 (see question 1.4 above) are: K Health, a developer of an AI-based personal health assistant; C2i Genomics, a developer of a liquid biopsy for cancer tumour monitoring; Viz.ai, a developer of AI-powered stroke care technology; Tyto Care, which developed a handheld device for on-demand remote medical exams; and Ibex Medical Analytics, a developer of cancer diagnostic software for use by pathologists.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

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.
- 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 the Helsinki Committee.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The following general regulations apply as well to digital health:

- 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.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The relevant laws applying to consumer healthcare devices or software are:

- As of December 2019, the Medical Equipment Act, enacted in May 2012, is not yet in force.
  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 charged with enforcing the regulatory schemes? 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?

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 3D medical image processing, simulation and design software or Neurosurgical Navigation Software.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

To date, no regulations applying specifically to AI have been enacted in Israel. Notwithstanding the above, digital health devices based on AI were registered in Israel by the Medical Accessories and Devices Department in accordance with customary guidelines applying to such devices abroad.

It is to be noted in this regard that the Israel Innovation Authority and the Ministry of Justice published in March 2021 a call seeking information from the public about the characteristics of the required regulations and the regulatory restraints in the field of AI, with an emphasis on the experimentation and the implementation of AI systems. In view of the above, one can assume that the Innovation Authority will issue a circular referring to the AI field.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  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 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.)
- **Clinical Decision Support Software**
  Clinical decision support systems are currently being developed by various start-ups in Israel. Today there is no regulation that sets conditions for the implementation of such systems. Some key issues are the need to convince physicians of the reliability of the system on the one hand and the need to prevent over-reliance on the system on the other hand.
- **AI/ML powered digital health solutions**
  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, namely, simulate professionals' behaviour, by using machine learning. 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.
- **3D Printing/Bioprinting**
  The three-dimensional printing field is a flourishing industry in Israel, used, *inter alia*, for the manufacture of hearing and surgical aids, dental models, physical models of organs as well as living cellular products and tissues, some of which are medically approved for human contact and transplantation.
  It is estimated that Israel is the manufacturer of approximately 40 per cent of all 3D printers worldwide, and more than 1,400 Israeli companies dedicated to life sciences. For example, the company Synergy3DMed designs and prints customised 3D models and surgical instruments. Recently, Tel Aviv University researchers used a 3D bio-printer to create a heart which includes real cells, blood vessels, ventricles and chambers. Another example is the collaboration between Israel's CollPlant Biotechnologies and the US-based United Therapeutics Corporation to begin the production of 3D-printed kidneys.
  While this technology significantly contributes to the development of healthcare, *inter alia*, by reducing global organ shortages, the different reactions of individuals to 3D-printed organ transplantations may raise an issue as to the efficiency of such organs.
- **Digital Therapeutics**
  We are not aware of any digital pills that were approved in Israel.
- **Natural Language Processing**
  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 2.1).

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 know-how products based on collaborations through which data is used; consideration for data sharing or know-how products based on use of the data, such as ownership in the outside organisation (if a company is concerned); right to use the know-how 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.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Even though the traditional intellectual property rights do not necessarily apply to data, the key legal issues regarding the securing of comprehensive rights are ownership and exclusivity in the use and collection of the data. For example, exclusivity in the use of data may be beneficial, and the manner in which the data is used is crucial in order to ensure an appropriate use, in accordance with the applicable regulations.

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 data requires informed consent, while sharing/disclosure of properly de-identified data does not.

Since the 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 which 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 of databases *per se*.

As of 2018, icons, graphical user interfaces ("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 rules or laws that apply to academic technology transfers in your jurisdiction?

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 licences and obtaining equity and/or royalties from commercialising products based on them.

Every academic institution has IP bylaws. Such bylaws bind the employees of the institution (including the researchers) by virtue of appropriate provisions in their employment agreements. Some institutions also require students to subject themselves to these bylaws. In general, academic institutions require ownership of any IP generated in the framework of the institution, and various provisions grant the inventors a certain share in the revenues of the academic institution's commercialisation company. It is common practice for the academic institutions that if the institution is not interested in patenting the technologies, then the inventors can own the IP in exchange for a revenue sharing agreement with the academic institution.

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).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

This question is being discussed in Israel in the framework of the examination of the patent applications nos 268604 and 268605, in which an AI machine ("DABUS") was listed as an inventor. A notice before rejection of each of the applications was issued on the ground that the applicant is not entitled to submit the applications, since he is not the inventor himself and did not derive title to the invention by operation of law, transfer or agreement with the inventor, since DABUS is not a legal entity and therefore has no capacity of having the right or transferring it. On June 21, 2021, the applicant filed a response arguing that DABUS can be listed as an inventor and that the applicant derives title from DABUS. The cases are currently awaiting the final decision of the examiner.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The Law for the Encouragement of Industrial Research and Development 5744-1984 sets forth the establishment of the Israel Innovation Authority ("IIA") (previously known as the Office of the Chief Scientist), which provides, *inter alia*, funding platforms to various entities such as early-stage entrepreneurs with technological initiatives, mature companies developing new products or manufacturing processes, academic groups seeking to commercialise their ideas and turn them into revenue generating products/services.

The State grants fundings, generally 50% of the capital required for the completion of the development plan including protection of IP. There is no need to return the fundings, unless the research generates revenues, and then the fundings are returned by way of royalties.

In addition, IP developed through fundings of the Israel Innovation Authority should be exploited in Israel and cannot be transferred to a foreign entity without receiving prior permission from the IIA.

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 details 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 the enforcement of foreground IP; and
- arrangements for revenue sharing of commercialisation of the collaboration results: royalty bases; rate; definition 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 healthcare and non-healthcare companies?

Agreements with public healthcare companies require special attention be given to the regulatory environment of the healthcare entity (e.g. a 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-licence 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 licence; 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 solutions?

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.

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-healthcare companies should consider before entering today's digital healthcare 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 healthcare ventures?

The arrival time of a large part of digital medicine technologies (such as smart apps and medical devices) is significantly short (unlike in pharmaceuticals 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 ("TTM") (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.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

There are no specific key barriers in Israel, but rather general key barriers that may be relevant in other jurisdictions as well and include, *inter alia*, the following: regulatory requirements in the targeted market (which are evolving and constantly taking shape and form), the characteristics of the targeted market/population, the need to cooperate with additional entities (strategic partners), etc.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The sole clinician certification body in Israel is the Ministry of Health. The decision whether to adopt digital health solutions is dependent on clinical benefit and cost-effectiveness, regardless of the technology.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

The Israeli market is different from the American market, since it is nationalised – namely, most of the health services are provided by HMOs, which are budgeted by the State. The services provided by the HMOs (including services, drugs, medical equipment and devices) are those that are included in the "health basket". The "health basket" is based on the health services that were being provided by the Clalit HMO as of January 1, 1994 and the health services that were provided by the Ministry of Health as of December 31, 1994. Once a year, new drugs and medical technologies are added to the "health basket" following approval by the MoH and subject to additional budgeting allocated for this purpose by recommendation of a public committee. The decision regarding which drugs and medical services are to be added to the "health basket" are made based on clinical benefit and cost-effectiveness, regardless of the technology. It is to be noted that some digital technologies, especially applications, are not regulatory defined as MAD (medical accessories and devices), which is a basic condition for the inclusion of a technology in the "health basket". Nonetheless, the "health basket" includes digital technologies such as CGM systems (continuous glucose monitoring) or smart pacemakers.

The health insurance market, however, is completely private, and each company determines the terms of the reimbursement.

Eran Bareket holds an LL.B. degree, 1990, from Tel-Aviv University and teaches in leading Israeli universities.
Eran's expertise is in litigation, in particular: IP-rights; unjust enrichment; competition law and complex litigations, particularly those involving technology issues; 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/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., Reinhold Cohn Group
26A Habarzel St.
Tel Aviv, 6971037
Israel

Tel: +972 3 567 2000
Email: eranb@gilatadv.co.il
URL: https://gilat-bareket.rcip.co.il

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., Reinhold Cohn Group
26A Habarzel St.
Tel Aviv, 6971037
Israel

Tel: +972 3 567 2000
Email: alcohen@gilatadv.co.il
URL: https://gilat-bareket.rcip.co.il

Reinhold Cohn Group (RCG) is the leading Intellectual Property consulting firm in Israel. RCG 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

Italy


Sonia Selletti


Giulia Gregori


Claudia Pasturenzi

Astolfi e Associati, Studio Legale

1 Digital Health

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

A legal definition is not provided by Italian law; however, "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 the World Health Organization (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 digital health technologies in your jurisdiction?

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 digital health for your jurisdiction?

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 (healthcare professionals (HCPs), healthcare organisations (HCOs), suppliers, producers, developers, patients, etc.), and wise liability management.

1.4 What is the digital health market size for your jurisdiction?

The COVID-19 pandemic has enhanced the value of "digital" solutions in every field. The continuing technological acceleration in the Italian healthcare system is part of a socio-economic context that had been moving along this path – albeit at a different speed – for years; a situation clearly reflected in the introduction of electronic health records or the first regulations governing telemedicine.

Given their potential as regards health safeguards and costs, it is reasonable to expect that digital solutions will become increasingly widespread over the next few years. This is also the direction taken by Italy's National Recovery and Resilience Plan, or PNRR (a document drawn up by the Italian Government to illustrate how it intends to manage the funds of the Next Generation EU programme set up by the European Union in response to the pandemic). The PNRR subdivides its interventions into six main missions, including digitisation, health and ecological transition), which provides for a substantial fund to be set up, on the one hand to strengthen so-called proximity networks, intermediate structures and telemedicine for territorial healthcare, and on the other to enable the upgrade and development of the existing technological and digital structures in the health sector.

Another important step towards the digitisation of Italy's national health system is the introduction of telemedicine to ensure the application of the criteria and reimbursement procedures set out in the so-called Essential Assistance Levels. The authorities have begun this process (although it is not yet completed) which is a central objective of their forthcoming actions.

In this context, it is vital that the development of digital health be accompanied by specific, uniform legislation guaranteeing appropriate regulation and support, so that all the potential offered by digital technology can be exploited in full.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

To our knowledge, the five largest digital health companies in Italy, in 2020, are Dedalus Italia S.p.A., GPI S.p.A., AB Medica S.p.A., Health Italia S.p.A. and Tesi S.p.A. (source: http://gpi.it/azienda).

We should add that the digital health ecosystem is also populated by numerous start-ups with innovative, high-performance proposals, who successfully obtain the approval, economic and otherwise, of other more structured organisations as well as of State/regional authorities to begin operating at territorial level.

In strategic terms, it is important that companies active in digital health form relationships with the public sector in order to establish essential public/private collaboration generating positive synergies. Public investment and private investment are a means to make the health service stronger.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

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 organisations 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 (mostly 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 core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

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 public administration that has seen the greatest growth in the use of new technologies, 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).

Furthermore, the current health emergency situation due to the pandemic has highlighted the need for the urgent implementation of digital media to promote remote healthcare services, given the restrictions on the movement of people and provisions on social distancing imposed at a national level. The competent authorities have put guidelines in place to provide stakeholders with guiding principles for the implementation and use of these technologies.

The digitisation promoted by the PNRR (see question 1.4) is the opportunity to create a more agile and efficient health system, and above all, a system with a greater focus on patient needs. To this end it will therefore be vital to establish regulatory schemes for optimal governance of the central elements where digitisation plays a key role, i.e.:

- development of telemedicine, to further enhance the potential of this tool which has already grown significantly during the COVID-19 health emergency;
- enhancement of data through Big Data Analytics, Artificial Intelligence and Machine Learning, to overcome existing fragmentation and take full advantage of the wealth of data held by various national, regional and local operators;
- enhancement, circulation and accessibility of the Electronic Health Record; and
- investment in digital skills, which are essential to sustain the cultural transformation of the system as a whole.

In any case, as regards digital health solutions, the application of more general laws, such as those relating to product safety, medical liability, medical devices, intellectual property is certainly important.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The wide expansion of mobile devices and apps with their software 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 (Regulation 2017/745/EU).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The main healthcare regulatory authorities in Italy are: the Ministry of Health, as the promoter and 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; and 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 Committee 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?

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 digital health 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, 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 governed by Regulation EU 745/2017 (the MDR) on medical devices (including active implantable medical devices), which has been applicable in Italy since 26 May 2021 (previously legislative decrees 46/1997 and 507/1992 applied as regards active implantable devices), and by Regulation EU 746/2017 (the IVDR), which governs *in vitro* diagnostic medical devices and will be applicable in Italy from 26 May 2022 (until then legislative decree 332/2000 applies). Full application of these European Regulations will, however, require the implementing decrees envisaged by Law 53/2021, which, in Art. 15, sets out the principles and guidance for the alignment of Italian legislation with the MDR and the IVDR.

That said, the first essential step is to ascertain if and when software falls within the definition of a medical device. The assistance of technical experts is advisable as well as careful evaluation of the legal profile: proper qualification will enable correct and effective market access.

For the purpose of correct juridical qualification of software, in addition to the above Regulations, it may be useful to refer to the "*MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (Eu) 2017/746 – IVDRr*" of the Medical Device Coordination Group (MDCG) set up in accordance with Art. 103 of the MDR (and pursuant to Art. 98 of the IDVR), whose aim is to help manufacturers establish when their software products qualify as medical devices.

More examples can be found in the "*Manual on borderline and classification in the Community Regulatory Framework for medical devices*" (version 1.22 of 2019). Still on the subject of medical device software, reference may also be made to:

- the "Guidance on Clinical Evaluation (MDR)/ Performance Evaluation (IVDR) of Medical Device Software" of the MDCG, March 2020;
- the "Guidance on Cybersecurity for Medical Devices" of the MDCG, December 2019; and
- the European Commission document "Is your Software a Medical Device?" (March 2021), which sums up the key steps for correct qualification of software.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

There are no specific regulations regarding artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use. When such instruments qualify as medical devices, the relevant regulations apply (*cf.* question 2.6). Otherwise, the distinguishing characteristics of each solution will have to be identified in order to establish the relevant regulations.

Useful pointers for contextualising the question are provided by the WHO guidance on Ethics & Governance of Artificial Intelligence for Health, drawn up as a result of deliberation amongst leading experts in ethics, digital technology, law, human rights, as well as experts from Ministries of Health. The guidance lists six principles to be followed to ensure that artificial intelligence operates in the public interest in all countries.

Additionally, on 21 April 2021, the European Commission presented a package (now being examined by the Council of the European Union) proposing harmonised rules on artificial intelligence and amendments to some EU laws, which could obviously have an impact on Italian legislation.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  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, which have seen a sharp increase as a result of the pandemic health emergency, with the implementation of remote consulting services in order to ensure the continuity of care for segments of at-risk populations (cardiology, cancer), apps to allow the rapid and immediate monitoring of patients in home surveillance, and inpatient remote monitoring kits (consisting of a smartphone and a Bluetooth pulse oximeter) in order to keep contact with health personnel to a minimum.
  Less recent is the use of telemedicine in the private sector. For example, this can include digital outpatient clinics that

provide digital platforms dedicated to telemedicine services through which telephonic and/or video consultations can take place with a specialised doctor and insurance companies, which integrate health coverage with telemedicine services. Telemedicine initiatives have received support from case law, which has recognised that non-purely health activities that pertain to broader telemedicine projects (such as the collection of health data through patient/technology interaction with subsequent sending to a physician for reporting) are not subject to the prior authorisation required by Italian legislation for the performance of healthcare activities (Supreme Court, criminal section, decision no. 38585/2019). This represented an important clarification for the development of new digital health initiatives.

- **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.
- **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.
  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, this software will 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. apps for measuring eyesight, apps 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.
  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.
  In order to manage the epidemiological emergency due to COVID-19, the Presidency of the Council of Ministers – Department for Digital Transformation, conceived and developed the "Immuni" mobile app for contact tracing, which helps to trace contacts that test positive for the pandemic through a notification system to other users of the app.
  As regards data processing, the Italian Authority for the Protection of Personal Data expressed important indications for their correct management (see question 4.1).
- **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.
- **Clinical Decision Support Software**
  Clinical decision support software uses technologies like Machine Learning, Natural Language Processing, and Big Data Analytics to assist physicians with clinical decision-making tasks, delivering actionable recommendations and providing complimentary materials like data reports, guidelines, clinical document templates and more.
  Consequently, the main issues are connected to liability profiles, should the clinical decision harm the patient, and the management and security of the personal data and information processed by the software.
- **AI/ML powered digital health solutions**
  A regulatory assessment of the context and rules to be applied may be necessary, depending on the type of activity covered by the digital health solution.

Relevant profiles include management and processing of personal data and correct identification of liability for damage arising from system errors or malfunctions. The outsourcing relationship requires a specific contract to govern these profiles.

- **IoT and Connected Devices**
  One of the main problems related to Internet of Things (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.
- **3D Printing/Bioprinting**
  3D printing is the technology that allows the creation of three-dimensional objects by joining or printing layers of material based on digital models. Among the main fields of application in healthcare is the production of medical devices, and is also used in the surgical field to recreate realistic models of organs to facilitate the understanding of complex surgical interventions. 3D printing can also be used to reproduce biological material for the replacement of human organs and tissues (bioprinting).
  The spread of 3D printing technologies in the healthcare sector certainly has an innovative scope that involves a multitude of corporate and professional entities. It faces many ethical and regulatory challenges, including the correct qualification of the systems in question (namely the applicability of legislation on medical devices), product safety, manufacturer and user responsibility, as well as the processing and protection of data collected by said systems and intellectual property. To date, the legal framework is still fragmented and the application of the rules remains uncertain.
- **Digital Therapeutics**
  As of the time of writing, there is no regulatory definition of Digital Therapeutics, but according to a definition proposed by the Digital Medicine Society – Digital Therapeutics Alliance (widely upheld by the scientific community), the concept includes software-controlled technologies that provide evidence-based therapeutic interventions to prevent, manage or treat a medical disorder or disease.
  Operating in a digital environment, Digital Therapeutics use a variety of techniques, ranging from simple reminders and calculations to gamification, cognitive behavioural therapy or virtual reality, in order to help patients' manage their clinical condition. The core issues concern correct qualification of Digital Therapeutics, which are hybrid solutions that present specific characteristics of medical devices but also affinities with pharmaceuticals. This also has implications as regards the national authorities responsible for the assessment of Digital Therapeutics. It is still not clear which regulatory authority (the Ministry of Health for medical devices or the AIFA for pharmaceuticals) should be responsible for the authorisation and management of these new therapeutic tools. Other questions to be considered are personal data privacy and security, and, depending on the type of technology and functions applied, risks relating to the safety of devices. Another complex issue is certainly the liability of the parties involved in the production, marketing and use of these solutions.
- **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 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 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 this 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.

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 (the "Privacy Code"), which can impose compliance with more rigorous obligations and requirements than those of other sectors.

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 Italian Privacy Authority "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*" of 16 November 2011).

Another critical issue is that of the identification of a legal basis suitable for legitimising the processing of health-related personal data as carried out through digital tools.

This issue emerged with particular reference to the contact tracing apps used during the COVID-19 health emergency as

a direct tool to detect contact amongst users of the app who tested positive for the virus (such as the "Immuni" app, see question 3.1). The Italian Privacy Authority has clarified that the health emergency does not automatically represent a legal basis for particularly invasive processing of data, such as the tracing of contacts by a public or private data controller. The only processing activities with an adequate legal basis are those based on national law and any other processing activities aimed at contact tracing are deemed to be carried out in violation of legislation on the protection of personal data.

Health facilities that equip themselves with telemedicine tools in order to comply with personal distancing measures to provide remote diagnoses or therapies are not required to request specific consent to the processing of the personal data as long as the data subject is provided with complete information with reference to the processing activities carried out.

On the other hand, since health facilities that process patient data through digital health services are dealing with special categories of data on a large scale, they should carry out a data protection impact assessment, in accordance with art. 35 of the GDPR (on this specific matter, see decisions no. 49 of 12 March 2021 and no. 201 of 13 May 2021, with which the Italian Privacy Authority assessed the GDPR compliance of two apps implemented by two different health facilities in order to enable patients' relatives to monitor the diagnostic condition of patients who access A&E).

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

The recent Decree Law 139/2021 (known as the "capacity decree") introduced changes to the Privacy Code, providing that processing by a public authority is always allowed if it is necessary for the performance of a task conducted in the public interest or for the exercise of the authority's public powers and that if the purpose of processing is not expressly envisaged under a law or regulation, it shall be decided and indicated by the authority consistently with the task conducted or the power exercised. The decree law also eliminated the requirement for the authority to consult the Italian Data Protection Authority before activating high-risk processing – for example, relating to health data.

Furthermore, 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 Italian 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 Italian 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 Italian 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 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 Italian Privacy Authority references to 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.

4.4 Do the regulations define the scope of data use?

A definition exists at neither a national 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 periodic audits.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The key legal issues with securing comprehensive rights to data relate not so much to the jurisdiction as to the means used to process data and to provide the information as at Arts 13 and 14 of the GDPR.

When personal data is processed through apps or other digital tools, the information required by the GDPR is not always

supplied in an adequate and sufficiently clear manner, partly because of the difficulties involved in making this information available in full and as smart information on these digital tools.

Furthermore, exercise of the rights envisaged by the GDPR must be guaranteed by making it easy for the data subject to forward requests to the data controller.

The data controller must enable the data subject to submit a request without the requirement of any particular formalities (for example, by registered letter, fax, email, etc.) and to this request, the data controller must provide an appropriate response within one month from its receipt (this period can be extended by two months, if necessary).

If the response to an application is not received within the indicated time frame or is not satisfactory, the data subject may contact the judicial authority or the Italian Privacy Authority.

Violation by the data controller of the provisions on the rights of the data subject is subject to administrative pecuniary sanctions of up to 4% of the total annual worldwide turnover of the previous year.

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 to 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 computer programs; 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.

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 rules or laws that apply to academic technology transfers in your jurisdiction?

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, licence, 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.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

The ownership of patents invented by artificial intelligence devices is a topical issue and is still being debated in a number of jurisdictions.

In 2019, the European Patent Office refused two applications indicating an AI system as the inventor on the grounds that the European Patent Convention requires the inventor to be a natural person. The applicant filed appeals against the EPO decision, which are still pending.

To date, there are no rulings on the matter.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The reference for government-funded inventions is Art. 65 of the IPC (see question 6.4) which applies to the inventions of researchers who work for a university or other public entity whose institutional purposes include research. Art. 65 of the IPC does not apply to research carried out within specific research projects funded by public entities other than the entity to which the researcher belongs.

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 healthcare and non-healthcare 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 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 solutions?

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 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 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 use maximum 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-healthcare companies should consider before entering today's digital healthcare market?

Non-healthcare companies must carefully know and take into consideration the healthcare sector rules and regulatory frameworks, among which, for example, are as follows:

- about the authorisation for the healthcare activity;
- about the relationships with HCP 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 in supporting the business model.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare 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 the others, is in constant evolution.

The market needs must then be analysed, while considering that the two main trends in the health sector consist of, on the one hand, unmet medical needs and, on the other hand, sustainability of the health system.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The main barriers are due to various factors, linked both to economic and organisational issues as well as the possibility of access to digital health solutions by healthcare professionals and patients.

In particular, digital health solution technologies involve costs that require the use of funds that public health facilities may not always have at their disposal.

Another key barrier is purely organisational, and depends on the autonomy of each region in its need to prepare resources and implementation tools. Organisational intermediation by the region appears necessary in order to obtain the structured configuration of the service, to define the procedures, competencies, and responsibilities of the structures and professionals involved, as well as the related costs. In Italy, this implies that the legislative-regulatory structure, organisational models, and the welfare strategies implemented for this purpose by the regions differ one from another, with consequent non-standardisation and fragmentation of the development and diffusion of these systems on a national level.

In addition, access to digital health solutions requires the availability of infrastructures (e.g., Internet connection) and devices (e.g., tablets and/or smartphones), to which some portions of the population of patients and healthcare professionals do not have easy access.

A further obstacle to the widespread clinical adoption of digital health solutions could be that regarding issues of health liability.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Italy there is no formal certification by medical associations in accordance with an objective protocol of criteria and without misleading claims.

At most, the endorsement of products by medical associations can take place. In order to be lawful, this endorsement must be accompanied by a certification of quality from passing a specific approval procedure, and not a mere commercial agreement, against payment, of product sponsorship by the association.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Italian law includes provisions guaranteeing the free supply of aids, equipment and prostheses for disabled patients (for example, made-to-measure ocular prostheses, acoustic equipment, corsets, wheelchairs, walking frames, incontinence catheters, etc.).

At the moment, there are no laws providing for reimbursement by the NHS or the free supply of apps or other digital solutions, but the question is certainly under discussion, considering that the growing spread of digital health tools requires the introduction of specific regulations to guarantee that patients have access to digital health solutions that provide them with clinical or therapeutic support.

In other words, the need is felt to identify which access and reimbursement models are usable and sustainable for the new digital tools, also because, besides the close attention paid to the creation of regulatory and clinical development procedures, consideration should be given to the fact that the generation of significant revenue flows is, and will be, one of the main challenges in this sector on all markets.

In this context, the orientation also among private insurers is to identify bespoke insurance packages that enable the user to choose personal prevention, diagnosis, treatment and convalescence services, which facilitate access to digital health solutions.

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 2 885 561
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 Astolfi e Associati 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 2 885 561
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 2 885 561
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 50 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

Japan


Mia Gotanda


Tomoaki Miyata


Kei Suzuki

GVA LPC

1 Digital Health

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

There is no clear definition of "digital health" in Japan. 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 artificial intelligence (AI) image diagnostic systems, software to indicate disease progression and others); (6) big data (medical, nursing, etc.); and (7) other businesses.

1.2 What are the key emerging digital health technologies in your jurisdiction?

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 given particular attention. There are many systems that utilise AI technology that includes medical applications, image diagnosis supporting systems, mental health tech, medical interview systems, and others. In addition, a recent amendment of the regulation for telediagnosis is receiving a lot of attention.

1.3 What are the core legal issues in digital health for your jurisdiction?

If a digital healthcare device 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.

1.4 What is the digital health market size for your jurisdiction?

The exact figure is not confirmed, but it is estimated to be around 800 billion yen as of 2017. The size of the digital health market is increasing every year and is expected to grow to about 1.2 trillion yen by 2025.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

In practice, many Japanese companies do not disclose their sales information. Considering that most Japanese companies offering digital health also offer other health-related products, information in revenue is not limited to the digital health domain. In addition, many venture companies in the digital health business also do not disclose their sales information. Therefore, the exact information on the ranking of digital health companies is unknown.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The core regulation applied to digital 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 licence 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 medical products), and which are specified by Cabinet Order". Medical devices are classified into four classes, depending on the risks to humans or animals. The approvals and licences also differ depending on each class.

Advertisements for medical devices that contain misleading information, etc. is prohibited. If the 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 core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The way in which personal information is handled can become 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 healthcare devices or software 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
(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 the 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 that mislead consumers in terms of quality, terms and conditions, etc.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? 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?

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 million yen.

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 million yen 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 2.25 million yen 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 million yen, 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.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

If AI/Machine Learning (ML) powered digital health devices or software solutions fall under "medical device" as defined in the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices, then it is subject to such Act in connection to manufacturing and sales. In addition, the Act on the Protection of Personal Information will also be applied in relation to the use of personal information.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  A medical practice licence is required to provide remote services using IT tools if such service is considered

"medical practice". Diagnosis and treatment are considered "medical practice", but the provision of general information is not considered "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 (physician), the propriety of such remote medical treatment becomes an issue because Article 20 of the Medical Practitioners Act requires physicians (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 physician gives medical treatments by following the guideline, it does not constitute a violation of the Act.

Further, based on the current COVID-19 pandemic situation, the Ministry of Health, Labour and Welfare provisionally mitigated the face-to-face diagnosis rules.

- **Robotics**
  If a robot falls under a "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 of the robot.
- **Wearables**
  With regard to wearable terminals, some of the issues that will come into question are whether or not (1) the wearable terminal measures and collects data, and (2) the program that analyses collected measurement data falls under "medical device".
  Please note that question 2.1 above describes the definition of a "medical device", and question 2.6 describes the applicability of software as a "medical device".
  For example, with regard to item (1), a program using a portable device with a built-in sensor to detect body motion is not deemed to be a "medical device", however, thermometers, hemo piezometers, and cardiac electrograms are considered "medical devices". Whether or not a wearable terminal is a medical device is dependent on the information which is to be measured or collected.
  With regard to item (2), a program that merely displays, transfers, and stores measurement data of an individual's health status only for health promotion, is not considered to be a "medical device".
- **Virtual Assistants (e.g. Alexa)**
  Virtual assistants are considered as mere supplementary tools to physicians; therefore, in general, it does not conflict with the Medical Practitioners Act.
  However, if the function of such supplementary tools 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.
- **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 described in question 2.6 above, then they are subject to laws and regulations. Please note that the information provided under "Mobile Apps" is also applicable.
- **Clinical Decision Support Software**
  Clinical Decision Support Software is considered mere supplementary tools to physicians; 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 its applicability as a medical device program as described in question 2.6 above, then they are subject to laws and regulations.
- **AI/ML powered digital health solutions**
  At the current technical level, AI/ML is not considered to be eligible to make definitive conclusions concerning patients' diseases, rather, it is considered a supplementary tool to physician service. In such consideration, a medical practitioner shall be responsible for making the definitive conclusion about a patient's diseases so that AI/ML shall not conflict with the medical practitioner licence as prescribed by the Medical Practitioners Act.
  AI/ML powered digital health solutions such as a "medical device" shall be considered in light of the applicable criteria for a medical device program, as described in question 2.6 above. Refer to Section 8 for more information about AI and ML.
- **IoT and Connected Devices**
  Similarly to Robotics and Wearables, the applicability of a "medical device" and product liability will apply to Internet of Things (IoT) and Connected Devices.
- **3D Printing/Bioprinting**
  Similarly to Robotics and Wearables, the applicability of a "medical device" and product liability will apply to 3D printing/bioprinting.
- **Digital Therapeutics**
  Digital therapeutics is essentially a medical device and is subject to the laws and regulations described in Section 2.
- **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 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 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.

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 the 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.

Please refer to Section 5 for the 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 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, and warranty and ownership of intellectual property rights, etc.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

If the data falls under "Personal Information" as defined under the Act on the Protection of Personal Information, it is very important to promptly notify the data subject of the purpose of utilisation, except if the purpose of utilisation has already been publicly announced. Most of the data collectors have their own privacy policy and the purpose of utilisation has already been publicly announced in such privacy policy. Therefore, establishing the appropriate privacy policy on the website is important.

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.

Please refer to question 4.1 for definitions of "personal information" and "special care-required personal information", and question 3.2 for the Act on Anonymised Medical Data Meant to Contribute to Research and Development in the Medical Field.

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

Please refer to 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 the 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 medical healthcare device program 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 rights, 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.

Additionally, 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 (an author or their 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, copyright commences at the time of the creation of the work and ends 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", are 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 are illegal.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

The laws and rules of intellectual property rights are important in this area.

The issue of ownership of an intellectual property right derived from research that has been conducted at a university (as to 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 commercialise the patent rights they own, the university often requests the company to pay the university a certain portion of the profits made from the commercialisation of the patent by the company ("non-exercising compensation"). Further, it is important to set conditions for publications concerning the patent in relation to the timing of such publication 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 the 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 as part of its contractual obligations, which are prescribed under Article 19 of the Industrial Technology Enhancement Act:

(1) in the case 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 the case where the national government finds it particularly necessary for reason of public interest and makes a request, making clear the reasons thereof, the contractor will grant the national government the right to use said intellectual property free of charge;
(3) in the case where the national government recognises that the contractor has not utilised the said intellectual property for a considerable period of time and does not find any justifiable grounds for such non-utilisation and when the national government finds it is particularly necessary for promoting the utilisation of said intellectual property and makes a request (making clear the reasons therefor), the contractor shall grant a third party the right to use said intellectual property as per instructed by the national government; and
(4) in the case where the contractor 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 the Cabinet Order, the contractor will need to 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 the Cabinet Order as being unlikely to hinder the utilisation of the said intellectual property.

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 steps may also be protected as a patent right.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

According to the Patent Act, an inventor shall be a natural person. Therefore, an AI device cannot be an inventor.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

In Japan, the Industrial Technology Enhancement Act sets the rules.

In the past, patents and other rights derived from government-funded research and development were owned by the national government.

However, in order to increase incentives for developers and promote the dissemination of the results of government-funded research and development, it has been decided that the organisation that conducted the research can obtain patent rights for the results of research commissioned by the national government, provided that the following requirements are met:

(1) The results of the research must be reported to the national government when they are obtained.
(2) To license the said intellectual property rights to the national government for no charge when the national government needs to do so for reasons of public interest.

(3) To license the said intellectual property right to a third party at the request of the national government when the said intellectual property right has not been used for a considerable period of time.
(4) To obtain the approval of the national government in advance for the transfer of the intellectual property right or the establishment or transfer of the right to use the intellectual property 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 healthcare and non-healthcare companies?

Manufacture and sale of products that fall under "medical device" prescribed by the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices. This 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 an ML 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 ML, and approval has been granted by the national government, additional approval may not be required for such improvements in the program, if the national government has, in advance, acknowledged the plan of such changes in the performance of the program.

8.2 How is training data licensed?

A licence is granted through the execution of contracts.

Training data is rarely protected 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 ML, belongs to the creator, in principle.

In principle, no one has any legal intellectual property right for the newly created algorithm from ML, 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 and 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 solutions?

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 where a physician makes a wrong diagnosis of someone's illness by using an AI program and the patient suffers damage, the physician shall be responsible for the damage, as the AI program is just providing assistance to the physician'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 the 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-healthcare companies should consider before entering today's digital healthcare 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.

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

As compared to other businesses, the healthcare business, especially for business related to a medical device that 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, which requires cautious business management.

Nevertheless, the 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.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

In Japan, there is a national health insurance system under which every Japanese citizen and a long-term resident must enrol to allow them to receive medical care with ease. In clinical practices, it is very important for digital health solutions to be approved as the authorised official health insurance treatments because only approved treatments may be offered to patients who seek to be provided with medical treatment within the national health insurance system.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Japan, the Ministry of Health, Labour and Welfare provides the certification of a medical device. In such certification process, the Pharmaceuticals and Medical Devices Agency verifies the quality, safety and efficacy of the medical device.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Since Japan has a universal health insurance system, patients can receive reimbursement for digital health solutions that are covered by the insurance. In order to be covered by the insurance, an application must be submitted to the Ministry of Health, Labour and Welfare, and approval must be obtained from the specialised organisation for insured medical materials and, depending on the category, from the Central Social Insurance Medical Council.

Mia Gotanda joined GVA LPC 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 LPC
EBS Building 3F
1-7-7 Ebisunishi, Shibuya
Tokyo
Japan

Tel: +81 3 6712 7525
Email: m.gotanda@gvalaw.jp
URL: www.gvalaw.jp

Tomoaki Miyata joined GVA LPC in 2020. He received his Bachelor of Law and *Juris Doctor* from Kyoto University and Kyoto University Law School, respectively. Before joining the firm, he worked as a legal officer in a company that develops disease prevention applications. Currently, as a practising attorney in the firm, he provides support to start-up companies that specialise in the technologies area, particularly in AI, IoT, telemedicine, and VR. His fields of expertise are digital health, corporate affairs, and finance.

GVA LPC
EBS Building 3F
1-7-7 Ebisunishi, Shibuya
Tokyo
Japan

Tel: +81 3 6712 7525
Email: t.miyata@gvalaw.jp
URL: www.gvalaw.jp

Kei Suzuki joined GVA LPC in 2017. Appointed as a Partner in 2020. His fields of expertise are business developing, mergers and acquisitions (M&A), corporate affairs and IT legal affairs. He has provided much legal support in cross-border transactions.

GVA LPC
EBS Building 3F
1-7-7 Ebisunishi, Shibuya
Tokyo
Japan

Tel: +81 3 6712 7525
Email: k.suzuki@gvalaw.jp
URL: www.gvalaw.jp

GVA LPC'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 LPC, 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

Korea


Joo Hyoung Jang


Ju Hyun Ahn


Ju Eun Lee


Caroline Yoon

Barun Law LLC

1 Digital Health

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

"Digital health" means the transformation of healthcare service to a digital environment.

1.2 What are the key emerging digital health technologies in your jurisdiction?

The key emerging technologies in the digital healthcare industry are big data, artificial intelligence, mobile healthcare and wearable devices.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital healthcare are regulations on telemedicine and protection of personal (medical) information.

1.4 What is the digital health market size for your jurisdiction?

The digital healthcare market in Korea is estimated to have been worth approximately 1.4 billion KRW in 2020. As Korea possesses a world-class 5G network and IT competitiveness, it provides a good environment for the digital healthcare industry to grow. Because the government is also adopting policies that actively foster the digital healthcare industry, the digital healthcare market in Korea is predicted to grow even more in the future.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

There is no official ranking of digital health-related companies. The development of start-ups in 2021 was remarkable, with a number of digital healthcare start-ups entering the stock market, and major conglomerates such as Kakao, Naver, Samsung Electronics, and LG also entering the digital healthcare industry.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

In Korea, digital healthcare is mainly regulated by the Medical Service Act. For example, telemedicine between medical personnel is permitted, but telemedicine between a medical personnel and a patient is prohibited in principle.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Other than the Medical Service Act, the main issue regarding digital healthcare is whether there is a violation of the Personal Information Protection Act.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Because the Medical Devices Act applies to the manufacture, import, and sale of medical devices, the issue is whether consumer healthcare devices qualify as medical devices under the Medical Devices Act.

Article 2 (1) of the Medical Devices Act defines a "medical device" as "an instrument, machine, apparatus, material, software, or any other similar product...used, alone or in combination, for human beings or animals[;]...[a] product used for the purpose of diagnosing, curing, alleviating, treating, or preventing a disease;...[a] product used for the purpose of diagnosing, curing, alleviating, or correcting an injury or impairment;...[a] product used for the purpose of testing, replacing, or transforming a structure or function;...[or a] product used for the control of conception".

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

In Korea, institutions such as the Ministry of Health and Welfare and the Ministry of Food and Drug Safety are in charge of digital healthcare-related affairs.

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

The Medical Service Act interprets the scope of "medical practice" broadly and stipulates that non-medical personnel cannot engage in medical practice, and medical personnel cannot engage in the medical business without establishing a medical institution under the Medical Service Act. Accordingly, there are broad restrictions on the digital healthcare businesses that non-medical personnel can undertake.

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

As stated earlier in question 2.3, according to the Medical Devices Act, the concept of "medical device" encompasses software, so if "Software as a Medical Device" also qualifies as "[a] product used for the purpose of diagnosing, curing, alleviating, treating, or preventing a disease;...[a] product used for the purpose of diagnosing, curing, alleviating, or correcting an injury or impairment;...[a] product used for the purpose of testing, replacing, or transforming a structure or function;... [or a] product used for the control of conception", the Medical Devices Act will apply to its approval.

2.7 What regulations apply to Artificial Intelligence/Machine Learning powered digital health devices or software solutions and their approval for clinical use?

For Artificial Intelligence/Machine Learning powered digital health devices or software solutions, if they qualify as "[a] product used for the purpose of diagnosing, curing, alleviating, treating, or preventing a disease;...[a] product used for the purpose of diagnosing, curing, alleviating, or correcting an injury or impairment;... [a] product used for the purpose of testing, replacing, or transforming a structure or function;... [or a] product used for the control of conception", the Medical Devices Act will apply.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Restrictions on telemedicine under the Medical Service Act, protection of personal information collected in the course of telemedicine, etc.
- **Robotics**
  Protection of personal information collected by robots, approval as medical devices, etc.
- **Wearables**
  Protection of personal information collected by wearable devices, approval as medical devices, etc.
- **Virtual Assistants (e.g. Alexa)**
  Protection of personal information collected by virtual assistants, approval as medical devices, etc.
- **Mobile Apps**
  Protection of personal information collected by mobile apps, approval as medical devices, etc.
- **Software as a Medical Device**
  Protection of personal information, approval as medical devices, etc.
- **Clinical Decision Support Software**
  Approval as medical devices, etc.
- **AI/ML powered digital health solutions**
  Approval as medical devices, etc.
- **IoT and Connected Devices**
  Protection of personal information collected by Internet of Things (IoT) and connected devices, etc.
- **3D Printing/Bioprinting**
  Protection of personal information of patients eligible for 3D printing, etc.
- **Digital Therapeutics**
  Approval as medical devices, etc.
- **Natural Language Processing**
  In the case of error, tort liability issues, etc.

3.2 What are the key issues for digital platform providers?

For digital platform providers, issues related to the Personal Information Protection Act and the Monopoly Regulation and Fair Trade Act are the main issues. For digital platforms, the enactment of a special law related to online platforms, the Fair Online Platform Intermediary Transactions Act, is being promoted in recognition that various harms are taking effect due to characteristics such as lock-in effect for consumers and network effect for suppliers.

4 Data Use

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

In Korea, matters related to the handling of personal information, such as collection, use, and provision, are regulated by the Personal Information Protection Act, and to handle personal information, the Personal Information Protection Act requires in principle the consent of the subject of the information.

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

If there are provisions regarding personal information in the Medical Service Act, the Medical Service Act takes precedence. For example, the Medical Service Act stipulates that medical personnel or workers at medical institutions may not disclose or publish the information of others that they come to know while conducting medical work, except as specifically provided for in the Medical Service Act or another act.

4.3 Which key regulatory requirements apply?

As explained above, data use is restricted by the Personal Information Protection Act and the Medical Service Act. In particular, the Personal Information Protection Act defines health-related information as "sensitive information" and stipulates that in principle, such information cannot be handled without receiving the separate consent of the subject of the information.

4.4 Do the regulations define the scope of data use?

Article 2, paragraph 2 of the Personal Information Protection Act defines the processing of personal information as "the

collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, searching, output, correction, recovery, use, provision, disclosure, and destruction of personal information and other similar activities". The Personal Information Protection Act separates collection and use of personal information from the provision of personal information and regulates them separately.

4.5 What are the key contractual considerations?

When conducting collaborative research, an important contractual consideration will be who owns the rights to that information.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The Personal Information Protection Act stipulates that the subject of the information may request that the manager of personal information correct, delete, or suspend handling personal information. If the behavioural information on the subject of the information generated and observed in the process of using the service pursuant to this purpose also qualifies as personal information under the Personal Information Protection Act, unless there are special provisions in other laws, the manager of personal information must comply with the request for correction, deletion or suspension of handling the personal information of the subject of the information.

5 Data Sharing

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

The information to be shared is reviewed to determine whether it qualifies as "personal information" or "sensitive information" under the Personal Information Protection Act, and if the information falls within either definition, the requirements under the Personal Information Protection Act must be met.

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

For medical institutions, the Medical Service Act takes precedence, and because the Personal Information Protection Act in particular strongly protects health-related information by defining it as "sensitive information", this should also be considered.

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

According to the Personal Information Protection Act, the manager of personal information may provide personal information on the subject of the information to a third party if the manager of personal information obtains the consent of the subject of the information or provides personal information within the scope of the purpose for which the personal information was collected.

6 Intellectual Property

6.1 What is the scope of patent protection?

Article 29 (1) of the Patent Act stipulates that an industrially applicable invention (highly advanced creation of technical ideas using the law of nature) is patentable, except for "[a]n invention publicly known or practiced in the Republic of Korea or in a foreign country prior to the filing of a patent application" or "[a]n invention published in a publication distributed in the Republic of Korea or in a foreign country or an invention disclosed to the public via telecommunications lines prior to the filing of a patent application". Article 94 (1) of the Patent Act states that "a patentee shall have the exclusive right to practice his/her patented invention for business purposes".

6.2 What is the scope of copyright protection?

Article 2 of the Copyright Act defines a "work" as "a creative production that expresses human thoughts and emotions". According to the Copyright Act, a copyright holder has moral rights (right to make public, right of paternity, and right of integrity) and economic rights (right of reproduction, right of public performance, right of public transmission, right of exhibition, right of distribution, right of rental, and right of production of derivative works) over his/her work.

6.3 What is the scope of trade secret protection?

Article 2, paragraph 2 of the Unfair Competition Prevention and Trade Secret Protection Act defines a "trade secret" as "information, including a production method, sale method, useful technical or business information for business activities, which is not known publicly, is managed as a secret, and has independent economic value".

A person who possesses trade secrets has the right to request prohibition of infringement of trade secrets and furthermore, may also hold liable a person who "damages the business interest of a person who possesses trade secrets through an intentional or negligent infringement of trade secrets" (Article 11 of the Unfair Competition Prevention and Trade Secret Protection Act).

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

Acts such as the Patent Act and the Copyright Act apply to academic technology transfer.

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

As a "computer program work", software is, in principle, protected by the Copyright Act, and if certain requirements are met, it may be protected as a patent by obtaining a patent pursuant to the Patent Act.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

As the Patent Act stipulates that the inventor or his/her successor has the right to obtain a patent for the invention, and

only natural persons are recognised as inventors. An artificial intelligence device cannot be the inventor of a patent.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The major laws related to national R&D projects (projects supported by a central administrative agency with budget or funds for R&D based on laws and regulations) are the Framework Act on Science and Technology and the Act on the Performance Evaluation and Management of National Research and Development Projects, etc. In addition, the Health and Medical Service Technology Promotion Act, the Basic Research Promotion and Technology Development Support Act, etc. may additionally be applied to individual departments.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

When signing an agreement for collaborative improvements, it is considered important to agree on the attribution, cost sharing, and profit allocation of intellectual property rights.

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

In practice, there may be areas where the boundary between healthcare services and "medical practices" regulated by the Medical Service Act is unclear. Therefore, it is necessary to review whether the pertinent healthcare service qualifies as a "medical practice".

8 AI and Machine Learning

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

Machine learning performs functions such as sensing and understanding data in combination with big data, and plays an important role in all areas of the healthcare industry, such as disease diagnosis, treatment, and development of new drugs.

8.2 How is training data licensed?

Issues regarding the licensing of training data is usually determined by an agreement between the parties. On the other hand, information can also be protected as a work or trade secret if certain requirements are met.

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

For algorithms that are improved by machine learning without human involvement, no conclusion has been established yet regarding to whom the intellectual property rights pertaining to the algorithm belong.

However, because the Patent Act stipulates that the inventor or his/her successor has the right to obtain a patent for an invention, accordingly, in the case of the above algorithm, it may be interpreted as meaning that no one has the right to obtain a patent for it.

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

When licensing data for machine learning purposes, the content, type, and person to whom the right to data belongs should be considered.

9 Liability

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

A person who provides medical services or manufactures medical devices may be liable for damages resulting from default or tortious acts.

9.2 What cross-border considerations are there?

In principle, the parties may choose the governing law by agreement between the parties, but protections granted to the consumer under the mandatory provisions of the country where the consumer's habitual residence is located may also be applied.

10 General

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

According to the Personal Information Protection Act, individual consent from the subject of the information is required to transfer personal information to a foreign company's cloud system. For this reason, there are cases in which a cloud system is introduced only for information that does not qualify as personal information.

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

As previously stated, the healthcare industry is subject to a high level of legal regulation, so non-healthcare companies need to review related legal regulations to enter the healthcare industry.

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

Key issues to consider before investing in digital healthcare ventures include regulatory risks and acquisition of intellectual property rights. For example, it may take a long time to obtain the relevant permits from the government.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

A key barrier holding back widespread clinical adoption of digital health solutions is the restrictions on telemedicine. Therefore, the current digital healthcare service remains mainly in the role of assisting in health management.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

All doctors in Korea are automatically enrolled in the Korean Medical Association as soon as they receive their medical licence. The Korean Medical Association, as an association representing the interests and rights of doctors, strongly opposes the use of telemedicine.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Digital healthcare is not eligible for insurance benefits under the National Health Insurance Act yet. In addition, digital healthcare is expected to be difficult to apply to health insurance in the near future due to the difficulty in measuring its value in the existing fee system.

Joo Hyoung Jang is the head of the corporate law group at Barun Law LLC. His practice focuses on cross-border transactions, M&As, and general corporate matters. He has accumulated a broad range of experience in the fields of cross-border transactions and M&As, and his representations include JP Morgan Chase & Co. in a litigation action and negotiations relating to derivatives linked to the Thailand baht with local financial institutions, Deutsche Bank on transaction of NPLs receivable from Jinro Group and the bankruptcy procedure of Jinro Group, KT Consortium on the acquisition of Kumho Rent A Car Co., Ltd., and CDL Co., Ltd. on the acquisition of the Hilton Seoul.
He has served as a Member of the Digital Media City of Seoul since 2003; and Vice-Commissioner of the International Committee of the Korean Bar Association and a Member of the In-House Lawyers' Special Committee of the Korean Bar Association since 2011.

Barun Law LLC
Barun Law Building, 92 gil 7, Teheran-ro
Gangnam-gu
Seoul 06181
Korea

Tel: +82 2 3479 7519
Email: joohyoung.jang@barunlaw.com
URL: www.barunlaw.com

Ju Hyun Ahn is currently a partner at Barun Law LLC. He received his M.D. from the School of Medicine at Pusan National University and his LL.M. from Kyushu University. He has served as a legal advisor to the Financial Supervisory Service and to Mokdong Hospital, which is affiliated with Ewha Womans University School of Medicine. His practice focuses on finance and medical care.

Barun Law LLC
Barun Law Building, 92 gil 7, Teheran-ro
Gangnam-gu
Seoul 06181
Korea

Tel: +82 2 3479 2449
Email: juhyun.ahn@barunlaw.com
URL: www.barunlaw.com

Ju Eun Lee received her B.A. from the Department of Economics at Seoul National University and her J.D. from Seoul National University Law School. She is currently an associate at Barun Law LLC.

Barun Law LLC
Barun Law Building, 92 gil 7, Teheran-ro
Gangnam-gu
Seoul 06181
Korea

Tel: +82 2 3479 5738
Email: jueun.lee@barunlaw.com
URL: www.barunlaw.com

Caroline Yoon is a Foreign Attorney at Barun Law LLC. As a junior member of the Corporate Advisory Group, she assists Korean and international clients on a broad range of corporate issues. She is also involved in the international arbitration practice at the firm. She received her B.A. in International Relations from Pomona College and her J.D. from USC Gould School of Law. She is a member of the California State Bar.

Barun Law LLC
Barun Law Building, 92 gil 7, Teheran-ro
Gangnam-gu
Seoul 06181
Korea

Tel: +82 2 3479 5790
Email: caroline.yoon@barunlaw.com
URL: www.barunlaw.com

Leader in Litigation
Barun Law LLC has achieved exponential growth since its establishment in 1998. It is recognised for its strength in litigation and assessed to be one of the major representative law firms of Korea. Such growth and development were possible due to Barun Law's continuous efforts in recruiting highly-trained professionals, close collaboration between partners and associates, strengthening of professional teams, and trust from clients who have experienced the firm's legal services.

Highest Quality Legal Service
Barun Law's dispute resolution and litigation practice is second-to-none in Korea; many of the firm's litigation partners are former judges or prosecutors. Based on the firm's competitiveness in litigation-related service, its corporate lawyers have achieved enormous growth as well, allowing the firm to provide the best-quality legal services in all practice areas.

www.barunlaw.com

BARUN LAW
법무법인(유한) 바른

Mexico


Abraham Díaz


Ingrid Ortiz Muñoz

OLIVARES

1 Digital Health

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, etc.).

Nevertheless, a definition generally accepted in Mexico – although in constant evolution – is that digital health is a concept that incorporates Information and Communication Technologies, into sanitary assistance products, services and processes, as well as into organisations and institutions that may improve the health of individuals.

1.2 What are the key emerging digital health technologies in your jurisdiction?

Many areas of digital health technologies are rapidly developing in Mexico, such as: portable and ingestible devices; mobile health apps; artificial intelligence (AI); robot health carers; medicine applied robots; 3D organ printing; blockchain; telemedicine; machine learning; genome research; drones; augmented and virtual reality; and electronic records and big data, among others. As stated above, these technologies are in constant evolution.

In relation to the above, the 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 digital health for your jurisdiction?

As a type of medical device aimed to be used by healthcare practitioners and patients, digital health 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 digital health. IT often involves the collection and/or transfer of data, and digital health could involve the collection and transfer of sensitive data. As a matter of fact, digital health is becoming more and more intrusive as it evolves, which is in itself a reason why the proper handling of personal information, especially the sensitive information, must be a core concern when dealing with new devices for digital health, thus having to bear in mind the concept of privacy by design. The mechanisms of data protection in Mexico are discussed further below.

It is advisable that entities offering digital health are aware of professional liability issues, and that they check whether their professional liability insurance covers events that may go wrong when providing digital health services, including providing services that require a medical licence or administering medical care.

1.4 What is the digital health market size for your jurisdiction?

The field of digital health is still relatively new in Mexico and its application in real life settings is still limited, however, it is rapidly growing, and the COVID-19 pandemic has certainly increased the rendering of remote health services, especially in the private sector. Additionally, due to the country size, Mexico is one of the most attractive markets in Latin America.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

The five largest digital health companies in Mexico are as follows:

- Eva.
- Zenda.
- Yana.
- Terapify.
- Sofía.
- Fundación Carlos Slim.

Please see the following for more information on the most prominent digital health companies in Mexico: https://wortev.capital/empresas-mexicanas-tecnologia-en-la-salud/.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

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; and
- 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 core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Since digital health implies health information management across computerised systems and the secure exchange of information between consumers, providers, payers and other suppliers and vendors, 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 healthcare devices or software 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.
- 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 Mexico there is no specific regulation concerning the sanitary approval of algorithms, apps, software, etc. that could be used as healthcare tools. So far, in practice, COFEPRIS reviews these products on a case-by-case basis. In general, these digital products are not considered medical devices as in most cases they do not have direct contact with the human body.

In addition, since consumer devices or technologies 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 charged with enforcing the regulatory schemes? 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 Data Privacy Authority (DPA) in Mexico. 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. INAI has the authority to conduct investigations, review and sanction data protection controllers and processors, 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 Bureau for Consumer's Protection (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".

At the beginning of 2021 PROFECO launched two initiatives in order to improve the self-regulation of e-commerce activities, which have boomed in Mexico as a consequence of the COVID-19 pandemic. The first one is the creation of a Code of Ethics for the regulation of e-commerce activities, and the second one if the grant of a digital trust seal, for those suppliers of online services who adhere to PROFECO's code of ethics, or who create a code of ethics that complies with PROFECO's guidelines, thus warranting a secure rendering of services for Mexican consumers.

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

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 UMAS (Unit of Measure for Sanctions) 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 *Fiscalía General de la República* (FGR) and the Customs Office in order to investigate and prevent counterfeit and illegal devices from entering the Mexican market.

In accordance with the Federal Law on Protection of Consumers, the PROFECO 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 of up to MXN25,000,000 (approximately USD1,400,000).

Additionally, there are two activities deemed as felonies related to the wrong use of personal information (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 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 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 (SaMD) and its approval for clinical use. As mentioned above, medical devices, a group under which digital technologies may currently fall, would require a marketing authorisation from COFEPRIS in order to be marketed and sold in Mexico.

So far, the regulations applicable to SaMD 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.

2.7 What regulations apply to Artificial Intelligence/Machine Learning powered digital health devices or software solutions and their approval for clinical use?

There are no specific regulations that apply to AI/Machine Learning (ML) powered digital health devices 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 AI/ML powered digital health devices 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.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**

  In Mexico, *telemedicine* is understood to include all aspects of incorporating information and communication technology (ICT) 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* telemedicine, 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.

  There is a proposal of amendments to the General Health Law. This initiative aims to implement telemedicine through electronic means. For this purpose, it suggests that both:

  - Medical prescriptions should be issued in digital form.
  - The provision of prescriptions in digital form should be implemented by public and private agencies as well as the organs of the National Health System, subject to any Mexican regulatory and official regulations issued by the COFEPRIS.

- **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 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 that 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 *telemedicine*, 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 SaMD 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. Additionally, copyright protection is available for software.
- **Clinical Decision Support Software**
  Initially, they might be considered as software, however, due to the purpose and health risks of this type of software, COFEPRIS will surely have to analyse the approval for the use of this technology in the health field.
- **AI/ML powered digital health solutions**
  In Mexico, the most recent development of AI/ML 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**
  Similarly to the above, applying internet of things (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.
- **3D Printing/Bioprinting**
  In the following years, 3D printing/bioprinting will provide the health sector with the possibility to print human organs. Currently, sections of bones are already being printed. Nowadays it is possible to print tissue with blood flow, but it is not yet approved for use. Evidence and studies are still needed to avoid risks for the population. Legislation in Mexico related to 3D printing/bioprinting is still pending, but it should be considered a medical device and should require marketing authorisation.
- **Digital Therapeutics**
  As explained for *mobile apps*, digital therapeutics developers or entities that deliver services through the same will need to be aware of any professional liabilities or licences required when providing digital therapeutics services or advice.
- **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 programme 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.
  - Confidentiality of information.
  - Cybersecurity and Business Continuity.
- 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 collecting of personal data, which concerning health issues constitute sensitive personal information; 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), and prior to the collecting of the personal data.

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 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.

Another key concern must be that if any digital health product or service implies the creation of a database including sensitive personal information, authorisation from the Mexican DPA (INAI) is required, and a Privacy Impact Assessment must be conducted.

As stated above, it is advisable to bear in mind the concepts of privacy by design and self-certification schemes when designing digital health products or services, in order to ensure that they are fully compliant with Mexican law.

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 any 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.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

It is highly important to guarantee the rights of the personal data used or collected, as to provide certainty to the users. Additionally, it is worth bearing in mind that any violation to such rights would be subject to a sanction in accordance with the applicable legislation. The Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations contemplate infringements and sanctions that might be imposed, previous rights protection procedure or the verification procedure carried out by the Institute.

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 Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations (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.

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 statutes, 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 49 of the Federal Law of Protection to the Industrial Property, the following subject matter is not patentable:

- inventions whose commercial exploitation would be contrary to public order or contravenes any legal provision, including those whose exploitation must be prohibited in order to protect the health or life of persons or animals, or to preserve plants or the environment;
- processes for modifying the germ line genetic identity of human beings and its products when they involve the possibility of developing a human being;
- uses of human embryos for industrial or commercial purposes;
- processes for modifying the genetic identity of animals which are likely to cause them suffering, without any substantial medical benefit to man or animal, and also animals resulting from such processes;
- plant varieties and animal breeds, except in the case of microorganisms;
- essentially biological processes for obtaining, reproducing and propagating plants and animals and the products resulting from such processes;
- methods for treatment of the human or animal body by surgery or therapy, as well as diagnostic methods;
- biological material can be patented if it is isolated or produced by means of a technical process; and
- the human body, at any stage in its formation or development, including germ cells, and the simple discovery of one of its elements or one of its products, including the sequence or partial sequence of a human gene.

Further, Article 47 of the Federal Law of Protection to the Industrial Property states that the following subject matter is not considered an invention:

- discoveries, scientific theories or their principles;
- mathematical methods;
- artistic or literary works or any other aesthetic creations;
- schemes, rules and methods for performing mental acts, playing games or doing business;
- computer programs;
- methods of presenting information;
- biological and genetic material as found in nature; 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.

These principles are recognised in domestic law, through the Federal Law of Protection to the Industrial Property.

The Federal Law for the Protection of Industrial Property foresees and regulates trade secrets. This new law includes

some changes, the most relevant one being the introduction of administrative infringement causes related to trade secrets, and the possibility of starting civil actions, before civil courts, aimed at collecting damages and losses derived from industrial property violations, including trade secrets.

This means that now the legal holder of trade secrets may attempt in Mexico either administrative, civil or criminal actions aimed at protecting its trade secrets.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

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 SaMD.

Software as such cannot be patented in Mexico, since it falls within the prohibitions of Article 47 of the Federal Law for the Protection of Industrial Property, 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.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

No, article 39 of the Federal Law for the Protection of Industrial Property establishes that the inventor, designer, or creator is presumed to be the natural person or persons indicated as such in the patent or registration application.

In this regard, an AI device is not considered a natural person, therefore, it could not be considered as a patent inventor.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

Mexico does not have any specific regulation related to government funded inventions, but applicable IP Laws and regulations, such as the Federal Law for the Protection of Industry.

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 in 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 healthcare and non-healthcare 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 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 AI 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 AI 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 solutions?

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, with the aim of being 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 and 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;
- 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-healthcare companies should consider before entering today's digital healthcare 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 healthcare 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 rapidly growing but on the private sector, while public hospitals are not receiving enough funds to make a big investment in digital health. Furthermore, 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 may 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: GDPR; the EU–US Privacy Shield; or any other future regulations substituting these. 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.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The principal key barrier holding back widespread clinical adoption of digital health solutions is that digital health is still relatively new in Mexico, and its application in real-life settings is still limited, so the legislation in this field is still developing in Mexico.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The key clinician certification bodies in Mexico are as follows:

- HealthTech Mexico Association.
- National Autonomous University of Mexico (UNAM).
- Mexican Foundation for Health (Funsalud).
- Tecnológico de Monterrey Health System (TecSalud).
- Mexican Association of Pharmaceutical Industry focused on Innovation (AMIIF).
- Mexican Association of Innovative Medical Device Industries (AMID).
- National Chamber of the Pharmaceutical Industry (CANIFARMA).
- Fundación Carlos Slim.
- There are some other bodies involved in the clinical adoption of digital health such as National Centre for Health Technology Excellence (CENETEC) and the National Council for Science and Technology (CONACYT).

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

So far, there are neither express nor specific rules concerning reimbursement for patients using digital health solutions.

However, in general terms, in the public sector there is no reimbursement, but the free services and products provided by such health institutions. Regarding the private sector, reimbursement can be done by and through private medical insurance, yet the specific rules regarding any formal certification, registration or other requirements in order to be reimbursed would be provided by such private companies.

Abraham Díaz "adds value for clients with diverse portfolios as a result of his tripartite copyright, trademark and unfair competition expertise", according to *World Trademark Review 1000*.

He is a Partner at OLIVARES, where he co-chairs the Litigation Team, and the Privacy and IT Industry group, and has a wealth of knowledge across all areas of intellectual property (IP), with a focus on copyright, trademarks, unfair competition, litigation, licensing and prosecution, as well as regulatory matters. He also counsels clients on trade dress, product configuration, advertising, false advertising, trade secrets, plant breeders' rights, vegetal varieties and Internet-related issues.

Mr. Díaz counsels multinational and domestic companies in industries such as technology and telecommunications, digital health and e-commerce.

He also provides guidance on the correct implementation, monitoring and auditing of privacy management programmes, as well as crisis and data breach management.

Mr. Díaz has authored articles on IP and Internet matters, as well as on privacy law, for leading industry publications and has lectured on cutting-edge IP topics in national and international fora.

OLIVARES
Pedro Luis Ogazón 17
San Angel
Mexico City 01000
Mexico

Tel: +52 55 5322 3041
Email: abraham.diaz@olivares.mx
URL: www.olivares.mx

Ingrid Ortiz Muñoz has a law degree from Tecnológico de Monterrey. She obtained a Master's/LL.M. degree in Intellectual Property from Bournemouth University, in the UK.

She is an Attorney-at-Law with more than 10 years of experience in the field, focusing on Intellectual Property Litigation, Administrative Law, Regulatory Law and Compliance; comprehensively advising national and transnational companies dedicated to innovation in the life sciences industry.

She has authored various articles published in Mexico and abroad on IP and the regulation of clinical research, pharmaceutical, biological, chemical, vaccine, agricultural, cannabis products, as well as medical devices, among others.

She participates in various national associations, including the Mexican Association for the Protection of Industrial Property (AMPPI), of which she is a member of the Regulatory Affairs Committee.

She is currently working in the firm's Life Sciences Group.

OLIVARES
Pedro Luis Ogazón 17
San Angel
Mexico City 01000
Mexico

Tel: +52 55 5322 3000
Email: ingrid.ortiz@olivares.mx
URL: www.olivares.mx

OLIVARES is continuously at the forefront of new practice areas concerning copyright, litigation, regulatory, anti-counterfeiting, plant varieties, domain names, digital rights, and internet-related matters, and the firm has been responsible for precedent-setting decisions in patents, copyrights, and trademarks.

- Patents.
- Trademarks.
- Copyrights.
- IP Litigation.
- Anti-Piracy & Anti-Counterfeiting.
- Civil Litigation & Commercial Litigation.
- Constitutional & Administrative Litigation.
- Alternative Dispute Resolution (ADR) & Mediation & Arbitration.
- Licensing, Tech Transfer & Franchising.
- Corporate and Commercial Law.
- Regulatory Law.

Our firm is committed to developing the strongest group of legal professionals to manage the level of complexity and interdisciplinary orientation that clients require.

We aim to utilise every available resource to help clients achieve optimum results, protecting their business interests, intellectual property and other rights at every level and through the applicable administrative or judicial venue, in order to maximise successful outcomes – all while maintaining an overarching goal of contributing to Mexico's broader stance in the global economy and for the greater good of the Mexican people.

www.olivares.mx

OLIVARES® we know MEXICO

Singapore


Gloria Goh


Koh En Ying


Tham Hsu Hsien


Alexander Yap

Allen & Gledhill LLP

1 Digital Health

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

Whilst there is no formal definition of "digital health" under Singapore law, the Health Sciences Authority ("**HSA**") has referred to digital health as "*the usage of connected devices, wearables, software including mobile applications and artificial intelligence to address various health needs via information and communications technologies*".

1.2 What are the key emerging digital health technologies in your jurisdiction?

The key emerging digital health technologies in Singapore are presently in the areas of artificial intelligence ("**AI**"), telemedicine, mobile health, data analytics and digitised and integrated healthcare systems. The Ministry of Health ("**MOH**"), amongst others, has recognised that AI is increasingly being used throughout the healthcare continuum in training, research, administration, clinical decision support and direct patient care.

Additionally, with the onset of the COVID-19 pandemic, platforms for teleconsultation and telemonitoring have come to the fore. There is increased integration of telemedicine into the national health management system to allow for improved patient management and reduced hospital visits and re-admissions.

In mobile health, mobile applications and wearable devices are used to monitor health statistics and wellbeing, and are used in conjunction with data analytic technology to identify trends and clusters based on proximity data (for example, the Trace Together mobile application / token developed for the COVID-19 pandemic).

Platforms for digitised and integrated health systems (such as the National Electronic Health Record, and the Health Hub mobile application) are also being implemented to facilitate the consolidation, digital management and sharing of patient's information and records across both the public and private sectors, to increase individuals' ease of access to the healthcare system.

1.3 What are the core legal issues in digital health for your jurisdiction?

The emergence of telemedicine as an increasingly popular way of delivering healthcare creates a need for regulation. At this time, telemedicine is mainly regulated by the National Telemedicine Guidelines (January 2015), and the Singapore Medical Council's ("**SMC**") Ethical Code and Ethical Guidelines (2016) ("**ECEG**") (amongst other *ad hoc* guidelines / advisories by various regulatory and professional bodies). Following a "regulatory sandbox" period for telemedicine and mobile medicine in which the MOH sought to better understand the risks of these service delivery models and co-create corresponding risk mitigation measures with the healthcare industry, and with the Healthcare Services Act 2020 ("**HCSA**") recently coming into force on 3 January 2022, the MOH plans to expand the scope of healthcare services regulation under the HCSA in phases. A statutory scheme for regulation of telemedicine is presently anticipated to come into force at about the end of 2023, and the planned licensable providers will be independent doctors and / or dentists offering teleconsultations themselves, as well as organisations which have set up clinical and operational governance for their doctors and / or dentists to provide teleconsultations. Until then, the MOH has published a list of such direct telemedicine service providers who have demonstrated awareness of the risks and benefits of telemedicine, have put in place measures to address the risks, and agreed to comply with the practice guidelines set out by the MOH. Indirect telemedicine providers (i.e. those who do not provide direct medical care, and only offer technology support such as platforms offering software-as-a-service for teleconsultation, directory listings, and payment solutions) will not be licensed.

Increasing development and marketing of digital health products and standalone software (i.e. software that is intended to function by itself, rather than to control or affect the operation of other hardware medical devices, also commonly known as "**Software as a Medical Device**" or "**SaMD**" in the context of the International Medical Device Regulators Forum ("**IMDRF**")) is also likely to raise issues of registration and licensing, specifically, an increased need to determine if digital health products and associated dealer activities require registration and licensing as a medical device under the Health Products Act 2007 ("**HPA**"), as well as the applicable risk classification (which in turn determines the applicable registration requirements). At this time, not all telehealth products are considered medical devices; for example, under the HSA's Regulatory Guideline for Telehealth Products (April 2019), wellness devices such as fitness trackers, with appropriate clarification statements as to the product's appropriate use, may be exempt from regulation as a medical device notwithstanding that their functions are in the nature of telemonitoring.

Within the existing regulatory regimes, there are also unique challenges posed by specific types of technology, such as AI / Machine Learning ("**ML**") and SaMD. The relevant regulators have begun to issue specialised guidelines, such as the Artificial Intelligence in Healthcare Guidelines (October 2021) ("**AIHGle**"), and conduct public consultations to determine

the appropriate requirements, such as the Consultation on the Regulatory Guidelines for Classification of Standalone Medical Mobile Applications (SaMD) and Qualification of Clinical Decision Support Software (CDSS) held in July / August 2021.

With increasing healthcare data stored and transmitted digitally, the security of patients' medical and health information is also of significant concern. Recent years have seen data breaches involving large amounts of confidential patient information, and fines totalling S$1 million being meted out by the Personal Data Protection Commission ("**PDPC**") to a healthcare provider and its information technology services provider.

Increased possibilities for healthcare to be delivered cross-jurisdictionally raises both jurisdictional and conflict of laws issues. The advent of electronic, consolidated patient information also raises questions as to the standards to which healthcare professions (in particular, public healthcare workers operating under time-poor conditions and in a team-based setting) ought to be held to when it comes to documentation.

1.4 What is the digital health market size for your jurisdiction?

We are not aware of definitive data on the digital health market size in Singapore.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

We are not aware of definitive data on the comparative revenue of digital health companies in Singapore.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The core healthcare regulatory schemes related to digital health in Singapore can be generally divided into regulation of digital health devices, healthcare service providers and healthcare professionals.

As regards devices used in the delivery of digital health solutions, health products (which include medical devices) are principally regulated by the HSA, a statutory board under the MOH, whose remit includes to regulate the import, manufacture, export and supply of medical devices in Singapore, and ensure that drugs, therapeutics, medical devices and health-related products are regulated and meet safety, quality and efficacy standards. The HSA administers and enforces the HPA and its subsidiary legislation, and also promulgates related guidelines. Telehealth products such as wellness devices that do not fall within the definition of medical devices are also subject to scrutiny by the HSA (see the Regulatory Guideline for Telehealth Products (April 2019)), although they do not generally require registration and licensing.

The regulation of healthcare services is overseen by the MOH, which is the government ministry responsible for monitoring the accessibility and quality of healthcare services provided in Singapore, providing health-related information and raising the general public's awareness on health issues. The regulatory regime for healthcare services is currently in a transitory state, moving from the incumbent premise-based system under the Private Hospitals and Medical Clinics Act 1980 ("**PHMCA**"), to the service-based system under the HCSA. The first phase of implementation under the HCSA commenced on 3 January 2022, and full implementation is currently expected to be at the end of 2023, likely alongside the repeal of the PHMCA. In addition, the national standards body, Enterprise Singapore, administers the Singapore Standardisation Programme through an industry-led Singapore Standards Council, whose standards cover new medical technologies, systems and processes, including telemedicine, personal care robots, and medical devices.

For further details as to the regulatory regime for telemedicine in particular, please see the response to question 1.3.

Finally, the healthcare professionals involved in the supply of digital healthcare are each regulated by their respective professional bodies. To name a few, doctors are regulated by the SMC under the Medical Registration Act 1997; nurses are regulated by the Singapore Nursing Board ("**SNB**") under the Nurses and Midwives Act 1999; and allied health professionals (such as physiotherapists) are regulated by the Allied Health Professions Council ("**AHPC**") under the Allied Health Professions Act 2011. Each professional body also typically promulgates its own code of ethics and / or ethical guidelines.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Other applicable core regulatory schemes include the personal data protection regime administered by the PDPC under the Personal Data Protection Act 2012 ("**PDPA**") and its subsidiary legislation (including the PDPC's Advisory Guidelines for the Healthcare Sector).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Medical devices (including software) for use by consumers are regulated under the HPA regime (overseen by the HSA) described in the response to question 2.1. Whilst consumer devices are not subject to a special regime of their own, the specific registration requirements that apply to a medical device can vary depending on the risk classification assigned to the device. Medical devices meant for consumer use are generally expected to be of lower risk, and would generally be subject to less stringent requirements. For example, consumer medical devices may be Class A (i.e. low-risk) devices and exempt from product registration.

There are also various general (non-health product-specific) regimes for the protection of consumers in Singapore, which would generally apply to consumers who purchase or use such consumer devices. For example, the Competition and Consumer Commission of Singapore administers the Consumer Protection (Fair Trading) Act 2003, which protects consumers from unfair practices by commercial suppliers (which would include suppliers of digital health devices). Consumers also generally have recourse to civil remedies against such suppliers under contract and tort law, and legislation such as the Unfair Contract Terms Act 1977 grant certain special protections to consumers, such as requiring the commercial supplier's standard terms of business limiting liability for breach to be reasonable before such terms will be valid against consumers.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

Please see the response to question 2.1.

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

The key areas of enforcement would generally mirror the areas of regulation in respect of medical devices, healthcare services and healthcare professionals, including registration, dealer's licensing, quality control, advertising, post-market obligations of record keeping and reporting, and the security of patients' medical and health information.

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

Where software falls within the definition of a medical device, this is regulated under the HPA regime described in the response to question 2.1. Such software includes software embedded in medical devices, standalone software (also known as SaMD), standalone mobile applications, and web-based software. The HPA and its subsidiary legislation, such as the Health Products (Medical Devices) Regulations 2010, set out the requirements for (amongst other things) registration, manufacturing, licensing and supply of SaMD. Unless exceptions (such as a special access route) apply, registration is generally required before the SaMD can be put to clinical use.

Key HSA guidelines relevant to SaMD include the Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach (April 2020) and the Regulatory Guideline for Telehealth Products (April 2019). The HSA has also recently conducted a consultation on draft Regulatory Guidelines for Classification of Standalone Medical Mobile Applications (SaMD) and Qualification of Clinical Decision Support Software ("**CDSS**") in July / August 2021, with the aims of harmonising the HSA's approach in determining the risk classification of SaMD with the IMDRF's guidance on SaMD and providing better clarity on the qualification of CDSS as medical devices.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

Where AI / ML powered digital health devices or software solutions fall within the definition of a medical device, these are generally regulated under the HPA regime described in the response to question 2.1. Particular guidelines have also been promulgated by the HSA which are relevant to AI medical devices, including Part 8 of the Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach (April 2020) and the AIHGle. Policymakers and regulators in Singapore have also articulated a technology- and sector-agnostic AI governance approach to the design, application and use of AI, known as the Model Artificial Intelligence Governance Framework (2nd ed., January 2020).

3 Digital Health Technologies

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

The following paragraph relates to the following technologies: telemedicine / virtual care; robotics; wearables; virtual assistants (e.g. Alexa); mobile apps; Software as a Medical Device; Clinical Decision Support Software; AI / ML powered digital health solutions; Internet of Things ("**IoT**") and Connected Devices; 3D printing / bioprinting; digital therapeutics; and natural language processing.

The following issues generally apply to all the above technologies: (i) categorisation of the relevant devices as medical devices under the HPA, and if so, determining the applicable risk classification (which has impact on registration and licensing requirements); (ii) data protection and security; and (iii) maintaining standards of healthcare that are comparable to traditional modes of delivery. Technologies which involve AI / ML and continuous learning capabilities, in particular, raise issues of post-market monitoring to ensure that learning does not compromise performance post-deployment.

Under the Cybersecurity Act 2018, acute hospital care services and services relating to disease surveillance and response have been identified as essential services. Therefore, information technology systems relevant to the provision of such services could potentially be designated as critical information infrastructure, and require compliance with the obligations under the Cybersecurity Act 2018.

3.2 What are the key issues for digital platform providers?

Please see the response to question 3.1.

4 Data Use

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

Key issues to be considered include transfers of personal data outside of Singapore (if the digital health technology provider stores personal data outside of Singapore), ensuring the security of users' personal data and the purposes for which personal data of users will be put to (beyond providing the service or product to users), for example, whether the personal data will be used for health / clinical research by a third party.

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

The considerations change if one entity is acting as a data intermediary (e.g. data storage provider) of another entity (e.g. product owner) that collects the users' personal data. A data intermediary is an entity that processes personal data on behalf of another entity under a contract. It has fewer obligations under the personal data protection regime and is only required to protect the personal data in its possession or under its control with reasonable security arrangements, cease to retain documents containing personal data (or remove the means by which personal data can be associated with individuals) if the purpose for which the personal data was collected is no longer served by the retention and there are no legal or business purposes for the retention and notify the entity that it is processing personal data on behalf of any occurrence of a data breach. In contrast, the entity for whom the data intermediary processes personal data is responsible for the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the entity itself.

4.3 Which key regulatory requirements apply?

The collection, use and disclosure of personal data must be in accordance with the personal data protection regime in

Singapore. The PDPA, its subsidiary legislation and guidelines (including Advisory Guidelines for the Healthcare Sector) issued by the PDPC, comprise the relevant regime for personal data protection in healthcare. The collection, use and disclosure of personal data must be with the consent of individuals (unless an exception applies) and for purposes that individuals have been notified of and a reasonable person would consider appropriate in the circumstances. Organisations must:

- permit individuals to obtain information on their personal data and the ways in which their personal data has been used within a year before the date of request and to correct their personal data;
- ensure that personal data of individuals is correct and complete;
- put reasonable security arrangements in place to protect personal data;
- ensure that personal data transferred outside of Singapore is subject to a standard of protection comparable under the PDPA; and
- notify the PDPC of data breaches in certain circumstances.

Under the Private Hospitals and Medical Clinics Regulations and the National Guidelines for Retention Periods of Medical Records (January 2015), there are also legal obligations regarding the retention of medical records.

4.4 Do the regulations define the scope of data use?

The regulations do not define the scope of data use. This depends on the nature of the digital health technology and the purposes for the collection, use and disclosure and whether users consent to the purposes. Having said that, there are certain purposes for which consent of users is not required and this list was expanded in 2021. Accordingly, if the scope of data use falls within such purposes, the regulations could be said to affect the scope of data use, assuming separate consent cannot be obtained.

4.5 What are the key contractual considerations?

The types of personal data collected, used and disclosed, the purposes for which the personal data collected will be used and disclosed, the parties to whom the personal data will be disclosed to should be clearly identified in obtaining consent from users. If there is to be any cross-border transfers of personal data, relying on contractual terms to comply with relevant data protection requirements is common, this should be considered when entering into / preparing the relevant contract.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Consent for purposes beyond that which is necessary to provide the service or product to users and which may not be considered appropriate by a reasonable person is one such key legal issue. Users need to be notified of these purposes and consent needs to be obtained (unless an exception applies) for these purposes, which may not be forthcoming from users. It is not permissible under the PDPA regime to require users to provide personal data beyond that which is reasonable for providing the service or product as a condition for providing the service or product. It bears noting that provided the above requirements are complied with, relying on consent for compliance with data protection requirements is fairly common.

5 Data Sharing

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

Whether the users have consented to the sharing of their personal data, the purpose for which the personal data is shared and whether any exceptions are applicable. If the sharing of personal data involves data transfers out of Singapore, the requirements for data transfers must be complied with. Please see the response to question 5.3.

Patient confidentiality is another key issue, and healthcare service providers and healthcare professionals need to be particularly cautious when allowing patients' medical information to be shared, including not to run afoul of ethical duties. For example, doctors need to be mindful of the provisions of the SMC's ECEG regarding medical confidentiality. Further, a breach of patient confidentiality could attract civil liability as a breach of confidence.

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

The considerations change if an entity is a data intermediary. Please see the response to question 4.2.

The sources, expression and nuances of the obligations of patient confidentiality may be different depending on the nature of the entities / persons in question (e.g. different professional bodies may articulate obligations of confidentiality differently), but the gist of the obligations are unlikely to vary hugely between healthcare service providers and healthcare professionals generally.

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

The purposes for which the personal data is shared must be notified and consented to by individuals. If the personal data will be shared with a recipient outside of Singapore, the transferring entity must ensure that the recipient protects the personal data with a standard of protection comparable to that under the PDPA. Please see the response to question 4.5 on relying on contractual terms in transferring data overseas.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patent protection is available for an invention that is new, involves an inventive step and is capable of industrial application. Under the patent examination guidelines, for computer implemented inventions, it must be established that said computer (or other technical) features, as defined in the claims, is integral to the invention in order for the actual contribution to comprise said computer (or technical features). Patents are protected for a period of 20 years from the date of application, once granted.

6.2 What is the scope of copyright protection?

Copyright protects expression of original works. Computer programs and software are literary works in which copyright can subsist. Copyright lasts for the life of the author plus 70 years (or 70 years after the year the work is first published if the author is not identified).

6.3 What is the scope of trade secret protection?

Trade secrets are protected through the law of confidence in Singapore. The protection of trade secrets are enforced through actions for the breach of confidence for any unauthorised access, use, referencing or disclosure. Trade secrets must be demonstrated to be information which is of a sufficiently high degree of confidentiality (e.g. secret processes of manufacture such as chemical formulae or special methods of construction) and not every piece of confidential information will constitute a trade secret.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

There are no laws that apply specifically to academic technology transfers in Singapore. The National IP Protocol may apply to academic technology transfers if the technology transfer takes place in the context of publicly funded research and development ("**R&D**") activities. Please see the response to question 6.7.

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

Copyright would protect the SaMD as a literary work. Whether patent protection is available depends on the scope of the invention and whether it fulfils the requirements of being new and involving an inventive step (the third requirement of being capable of industrial application would be satisfied).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

This issue has not yet been tested before the Singapore courts. There is case law that interprets "inventor" under the Patents Act 1994 as being a natural person.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

There are no laws that apply specifically to government-funded inventions in Singapore. However, the National IP Protocol applies to all public agencies and R&D activities funded by public agencies. It sets out a general framework and principles for how intellectual property ("**IP**") arising out of public agencies / publicly funded R&D activities should be owned, protected, used and commercialised. It states that public agencies should generally reserve a royalty-free, irrevocable, worldwide, perpetual and non-exclusive right to use any licensed or assigned IP for their statutory functions, non-commercial and / or R&D purposes. Public agencies should consider the commercial interest of the third party before applying this principle and act in a manner that supports the effective commercialisation of the IP by the third party. Commercialisation of IP created using public funds should also benefit the researchers who are the inventors or creators of the IP.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Singapore law allows parties to determine *inter se* the ownership of intellectual property in collaborative improvements. While parties generally gravitate towards some type of co-ownership, and setting up a regime for this is possible as a matter of law, we would generally suggest that parties designate a single owner.

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

No special considerations apply, beyond the need for the healthcare company to comply with its usual regulatory obligations (and to check if any are specifically triggered by the agreement in question).

8 AI and Machine Learning

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

ML (and AI, more generally), when incorporated successfully into clinical workflows, can play roles in:

- enhancing communications (e.g. through natural language processing with foreign patients);
- improving efficiency, accessibility, quality of diagnosis and triage (e.g. through pattern recognition of radiological images); and
- improving recommendations on interventions (e.g. through the accumulation and analysis of data tuned to the local population and context, which in turn enables more accurate prediction of health risks and outcomes).

8.2 How is training data licensed?

Training data is typically provided by one party to another under contract. The terms vary between parties and the nature of the projects or purposes for which training data is licensed. Training data may be protectable by copyright as a compilation but no copyright subsists in the data itself. There is no *sui generis* database right in Singapore. Parties commonly rely on contractual obligations (including obligations of confidentiality) to control use of 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?

This issue has not yet been tested before the Singapore courts. Current case law requires that there must be a human author identified before a literary work will be an original work in which copyright subsists. Works created by humans with the assistance of AI may be protectable by copyright on the basis that the human is the author.

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

Common commercial considerations include the value of the data (e.g. whether other third parties have similar data) which may have an impact on whether the party providing the data can negotiate for any rights to any IP / value that is generated through the use of the data for ML. Since no IP subsists in data (except as a compilation, provided the compilation was created through the application of intellectual effort, creativity

or exercise of skill or judgment), protecting the use of data by the receiving party through contractual restrictions and obligations (including confidentiality) is important.

9 Liability

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

In Singapore, liability for adverse outcomes in digital health solutions is typically based on tort or contract law. For example, actions for injuries caused by use of faulty digital health products are typically founded on the tort of negligence, which requires that the elements of negligence (i.e. a duty of care, breach of the standard of car, causation and damage that is not too remote) be proven. Further, actions for breaches of patient confidentiality could amount to the tort of breach of confidence.

In addition, a contractual claim may lie if a contractual relationship exists between the claimant and defendant, and the adverse outcome arises due to breach of term of a contract and / or the contract prescribes remedies for the adverse outcome.

9.2 What cross-border considerations are there?

Increased popularity of digital health solutions, gives rise to the increased potential for cross-jurisdictional delivery of healthcare (e.g. through telemedicine) or cross-jurisdictional manufacture or marketing of digital health equipment. This raises questions of, amongst others: (i) the proper forum for pursuing a claim; (ii) the applicable law for the purposes of determining liability if an adverse outcome occurs; and (iii) enforcement of any award / judgment where a defendant's assets are situated in a foreign jurisdiction.

10 General

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

Cybersecurity and data protection (in particular where electronic health records of patients are involved) issues apply equally for Cloud-based services for digital health. Please see the responses to question 3.1 and sections 4 and 5.

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

Depending on the manner of entry, there may be additional regulatory requirements, such as those highlighted in our responses above.

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

The healthcare industry in Singapore is a highly regulated space, and specific regulations / requirements may apply depending on the precise operations / transactions in play. Venture capital and private equity firms should consider and seek advice on the relevant regulations (including the need for due diligence on potential regulatory exposure) before investing in digital healthcare ventures in Singapore. Depending on the technology involved and the area of application in digital health, it may also be necessary to consider freedom-to-operate searches to assess third-party IP infringement risks and whether sufficient steps have been taken to protect IP rights that may subsist in the digital health solution.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Digital health solutions are increasingly available in Singapore, including as a way of managing the challenges posed by the COVID-19 pandemic. However, key challenges for widespread clinical adoption of digital health solutions include:

- Costs of digital transformation: Costs may include initial set up costs and costs of maintaining digital systems, as well as employee training, creation of compliance strategies and the implementation of security measures to protect data.
- Singapore's ageing population: Many elderly Singaporeans remain unfamiliar with technology and digital health solutions, and training programmes / outreach efforts may be costly.
- The inability of digital health solutions to replicate the compassion and empathy associated with the healthcare profession: Patients may prefer the face-to-face interactions of visiting their doctor or healthcare professional.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Clinician certification bodies (such as the Specialists Accreditation Board under the Medical Registration Act 1997) do not routinely have the clinical adoption of digital health solutions as a focus. This is more likely to be influenced by the prevailing government policies (and the work of bodies as such the Smart Nation and Digital Government Office, and its implementing arm, the Government Technology Agency) as well as sentiments of healthcare professionals and the public, and practical issues such as the costs of implementation.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Patients who use digital health solutions in Singapore can be reimbursed by government insurers or private insurers. For example, the MOH has published a Table of Surgical Procedures, which lists microsurgical reversal of sterilisation by robotic means as a procedure in respect of which claims under MediShield Life (a basic health insurance plan administered by the Central Provident Fund Board) may (up to certain maximum claim limits) be made. Details of the extent to which reimbursement will be provided and the requirements for reimbursement, including whether there are any requirements on the digital health solution provider, would depend on the specific coverage agreed for between the insured and insurer.

Acknowledgments

The authors would like to thank Sophia Eliza Rossman, Associate, and Charlotte Wang, Associate, at Allen & Gledhill LLP, for their valuable assistance in the preparation of this chapter.

Gloria Goh's areas of expertise are in intellectual property, technology and pharmaceuticals, health products, cosmetics and food regulation. Her practice involves a broad range of contentious and non-contentious matters involving trade mark, copyright, patent, domain names, confidential information and data protection. Her experience includes conducting intellectual property due diligence in corporate transactions, conducting intellectual property audits for clients, advising clients on the acquisition of intellectual property and drafting and negotiating commercial agreements relating to the acquisition of intellectual property.

Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7568
Email: gloria.goh@allenandgledhill.com
URL: www.allenandgledhill.com

Koh En Ying specialises in litigation and dispute resolution, with a focus on medical malpractice and construction disputes. In relation to the former, she regularly deals with medical negligence claims, disciplinary proceedings and coroner's inquiries, and has advised and represented a medico-legal defence organisation, insurers, healthcare professionals and hospitals in matters across a range of general and specialist medical practices. Her practice also includes advising on medical regulatory issues, such as the regulation of healthcare professionals, healthcare service providers, and health products, including, where relevant, to operational matters and corporate transactions.

Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7507
Email: koh.enying@allenandgledhill.com
URL: www.allenandgledhill.com

Tham Hsu Hsien's main areas of practice are in healthcare and professional indemnity, banking and employment litigation, and insolvency and restructuring. In the area of healthcare and professional indemnity, he advises professional indemnifiers, insurers, and healthcare providers on regulatory and litigation matters. His contentious practice includes malpractice litigation and disciplinary proceedings.
His non-contentious practice includes advising healthcare providers on regulatory and contractual issues, and advising insurers on localisation of insurance policies. He regularly contributes to healthcare industry education and healthcare legislation consultations. He also sits on the Ministry of Health's Transplant Ethics Committee. He also advises major banks and corporates in Singapore in commercial disputes, with a focus on restructuring and insolvency, employment, and banking matters. He is fluent in written and spoken Mandarin, and has acted regularly for Chinese clients in commercial litigation and arbitration.

Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7820
Email: tham.hsuhsien@allenandgledhill.com
URL: www.allenandgledhill.com

Alexander Yap is Co-Head of the FinTech Practice at Allen & Gledhill. He focuses on the acquisition, divestiture, provision, sharing or receipt, of technology and intellectual property-related assets, data and services.
He also advises on intellectual property licensing, R&D and sponsorship arrangements, cybersecurity, collaboration agreements, outsourcing, distribution and franchising, online gaming, the cloud and "as-a-service" platforms, and is a key contact for data protection & privacy compliance matters and data breach management. Alexander was recommended for his expertise in intellectual property work by *The Legal 500 Asia Pacific 2019* which notes him as "a key name for commercial transactions relating to intellectual property, information technology and the protection and management of data".

Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7627
Email: alexander.yap@allenandgledhill.com
URL: www.allenandgledhill.com

Allen & Gledhill is an award-winning full-service South-east Asian law firm providing legal services to a wide range of premier clients, including local and multinational corporations and financial institutions. The Firm is consistently ranked as a market leader in Singapore and South-east Asia, having been involved in a number of challenging, complex and significant deals, many of which are the first of its kind. The Firm's reputation for high-quality advice is regularly affirmed by the strong rankings in leading publications, and by the various awards and accolades. With a growing network of associate firms and offices, it is well-placed to advise clients on their business interests in Singapore and beyond, on matters involving South-east Asia and the Asian region. With its offices in Singapore, Myanmar and Vietnam, as well as its associate firm in Malaysia (Rahmat Lim & Partners), and its network firm in Indonesia, Soemadipradja & Taher, Allen & Gledhill has over 650 lawyers in its network across the region, making it one of the largest law firms in South-east Asia.

www.allenandgledhill.com

ALLEN & GLEDHILL

Spain

Baker McKenzie

Montserrat Llopart

1 Digital Health

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 digital health technologies in your jurisdiction?

Telehealth is increasingly taking hold and making interactive, real-time communication between patients and healthcare professionals commonplace, avoiding the need for face-to-face medical visits. In Spain, all interested stakeholders are investing in this area: the national health service, private insurance companies and telecommunications companies that partner with established telehealth providers.

Besides, the shift from treatment to prevention in healthcare and the rise of patient-centric solutions has boosted innovation in the field of digital health and wellness monitoring, with the development of a wide array of health apps and mobile and wearable devices.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues are data privacy, quality of data, cybersecurity and the interoperability of IT systems as well as IP rights. Regulatory issues (product classification as medical device) and financing are also key for the development of digital health.

1.4 What is the digital health market size for your jurisdiction?

The pharmaceutical industry in Spain generated revenues of more than 22,000 million euros in 2020. There is no data on the digital health market size for Spain.

The SEIS index, created by the Spanish Society of Health Informatics in collaboration with the Health Ministry and the public entity Red.Es, evaluates and quantifies the implementation of Information and Communication Technologies (ICTs) in the Spanish public health system. Data from 2020 shows that the overall expenditure on technology platforms and information systems increased by 8.09% and 17.14% respectively in comparison to 2019. It also shows that tele-dermatology, tele-ictus and tele-ophthalmology are among those telemedicine specialities with the most initiatives. Finally, some of the most prioritised ICT projects undergoing implementation relate to data analysis and knowledge generation, production of population-based information to support clinical decision making, health personnel channel, electronic health records and health portals.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

The Spanish digital healthcare market is characterised by a high fragmentation of its operators, consisting of three main groups: start-ups; pharmaceutical companies with digital health initiatives; and ICT/technology companies investing in digital health or partnering with healthcare players.

The market is rapidly changing with the entrance of new start-ups. The most relevant private equity funding company in digital health for 2020 was Savana (15 million euros), which develops artificial intelligence (AI) and big data in order to unlock the clinical value embedded within electronic medical records (Deep Real World Evidence).

Well established pharmaceutical companies, such as Roche, Abbot, Medtronic or Almirall, are developing and/or have already implemented digital health solutions.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Spain does not have specific legislation relating to digital health, but the following schemes apply:

- Royal Legislative Decree 1/2015, approving the revised text of Law 29/2006 on Guarantees and the Rational Use of Medicines and Medical Devices.
- Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices (applicable as of 26 May 2022).
- Royal Decree 1591/2009 on medical devices; Royal Decree 1616/2009 on active implantable medical devices; Royal Decree 1662/2000 on *in vitro* diagnostic medical devices (currently all of them under review to adapt them to the above EU Regulations).

- Law 34/1988 on Advertising.
- Law 3/1991 on Unfair Competition.
- Guide for Advertising of Medical Devices to the General Public of the Catalonia region – January 2017.
- Code of Ethics of the Spanish Board of the Medical Associations (OMC).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The following regulatory schemes apply to digital health in Spain:

- 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 regulating the National Security Framework in the field of e-government.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The following regulatory schemes apply to consumer healthcare devices/software in Spain:

- Royal Legislative Decree 1/2007 approving the revised text of the general law for the protection of consumers and users (GLPCU).
- Royal Decree 1801/2003 on general product safety.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The Ministry of Health, Consumer Affairs and Social Welfare is responsible for the financing of 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, attached to the Ministry of Health, supervises the whole lifecycle of medical devices.

The regional authorities are responsible for the provision of healthcare services, supervision of promotional activities, enforcement of consumer protection and market surveillance in general.

The Spanish Data Protection Agency is the national supervisory authority under the GDPR and ensures that data privacy principles and regulations are respected.

The Spanish Board of Medical Association is responsible for supervising doctors, including telemedicine practices.

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

The key areas of enforcement for digital health in Spain are the following:

- Regulatory authorities' actions against digital health and healthcare IT that meet the definition of medical devices but have not obtained the CE mark.
- The Spanish Data Protection Agency's 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.

EU Regulation 2017/745 is fully applicable whereas Regulation 2017/746 will remain in a transitional situation until 26 May 2022. At Spanish level Royal Decree 1591/2009; Royal Decree 1616/2009; and Royal Decree 1662/2000 (currently all of them under review to adapt them to the above EU Regulations).

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.

Digital solutions to be adopted by the national health service are checked to ensure that the security standards required for the public administration are met.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

AI in healthcare is mainly regulated by the EU Medical Devices Regulation 2017/745 (MDR) and In-vitro Diagnostic Medical Devices Regulation 2017/746 (IVDR) in combination with the GDPR. Medical devices are often either developed using AI or they have an AI component. GDPR applies since the application of AI implies the collection or treatment of data, and, specifically health data, which is considered as special category data and is subject to strict privacy and data protection obligations. MDR and IVDR contain both *ex ante* and *ex post* requirements for AI in healthcare to be safe and performant throughout their entire lifecycle.

Moreover, Ethics Guidelines for Trustworthy AI, published by the European Commission (2019) highlighted that AI applications should not only be consistent with the law, but they must also adhere to ethical principles and ensure their implementations avoid unintended harm.

On a European level, the European Union has presented a Proposal for Regulation, laying down harmonised rules on AI (Artificial Intelligence Act), that will impact medical device and diagnostic companies. Regulation classifies medical devices and *in vitro* diagnostics as high-risk AI systems, therefore those AI systems will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the Union market. Predictable, proportionate and clear obligations are also placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle. Importance of this Regulation also lies in the fines for non-compliance, some of them up to 30 million euros or up to 6% of the total worldwide annual turnover for the preceding financial year.

In Spain, following the European scheme, the applicable legislation would be the Royal Decrees regulating medical devices, implantable medical devices and *in vitro* diagnostic medical devices, as well as Organic Law 3/2018 on the Protection of Personal Data (DPL).

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  There is no specific telemedicine regulation in Spain. Regulatory loophole was a problem itself because the legislation governing the healthcare professions refers to the medical profession's deontological rules and the Code of Ethics of the Spanish Board of Medical Association rules out telemedicine, unless ancillary to the face-to-face medical consultation. Privacy is another important concern, especially consent, data minimisation and data security.
  As for virtual care, covering both clinical and non-clinical applications, key issues relate to privacy and cybersecurity.
- **Robotics**
  The core issues are product qualification, 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, product qualification and 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. Additional concerns relate to the illegal non-licensed practice of medicine if enforcement authorities consider that the virtual assistant is giving medical advice.
- **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.
- **Clinical Decision Support Software**
  Lack of interoperability between different systems and the difficulty to pool information from many and diverse clinical sources. Moreover, product classification and privacy issues.
- **AI/ML powered digital health solutions**
  Product qualification and liability issues in the event that the algorithm fails and triggers a faulty clinical decision. As long as the product liability framework is not amended, the chances to get a developer of a standalone software liable for defective product are limited.
- **IoT and Connected Devices**
  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.
- **3D Printing/Bioprinting**
  Product qualification of the resulting product. The collection of biological samples intended to be used for 3D printing/bio printing in the framework of biomedical research is subject to Law 14/2007, especially with regards to informed consent, confidentiality and personal data protection. In addition, liability issues could arise with regard to implanted bio artificial organs or tissues.
- **Digital Therapeutics**
  Sound evidence of performance and clinical evidence is key for digital therapeutics (DTx) to receive conformity assessment under the medical devices regulation. Furthermore, risks pertaining to data protection refer to the profiling of patients and the serious security threats and major consequences in the event of a data breach.
- **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 Spanish 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, Internet of Things (IoT), medical devices and other digital healthcare technologies without compromising the integrity of the platforms.
- Market access issues due to the need for validation before connecting with 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 (art. 9 GDPR) and that 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.

The first step when using personal health-related data is to clearly define for which purposes the personal data will be used, in order to check if any of the exceptions foreseen in art. 9 GDPR apply and to be compliant with the transparency principle. In this regard, it is usually 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 shall limit the purposes for which personal data is collected and provide transparent and granular information on how and by whom personal data is going to be processed. Extending the types of processing in the future to purposes not foreseen at the outset or that could have appeared with the evolution of the market may not be compliant with the transparency principles of the GDPR, and the obligations of privacy by design and should 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.

4.3 Which key regulatory requirements apply?

When using personal health-related data, appropriate safeguards are required. These include, for example: (i) correctly identifying 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.

Pursuant to art. 37 of the GDPR, the controller and the processor shall designate a data protection officer in the following events: *inter alia*, if the processing is carried out by a public authority or body, or if core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to art. 9 (e.g. data concerning health). Under Spanish data protection legislation (art. 34 SDPL), in addition to the circumstances foreseen in the GDPR, there are some entities which shall designate in any case a data protection officer, such as entities operating networks and providing communications services when dealing with habitual and systematically personal data on a large scale; or healthcare centres legally required to maintain patients. Digital health providers should generally process personal health data on a large scale, and therefore they will be obliged to designate a data protection officer.

In addition to the above, other regulatory requirements which stem from the treatment of personal health data are the following: (i) regardless of the size of the entity, the controller, or if applicable the processor who processes health data on behalf of the controller shall keep a record of processing activities pursuant to art. 30 GDPR; and (ii) by default, when there is large-scale processing of health data, the controller shall carry out a data protection impact assessment pursuant to art. 35.3 GDPR.

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. 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 personal data under art. 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. 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?

(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. 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 to pseudonymised data in order to reveal the identity of the data subjects.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Health data is categorised as a special category of data according to the GDPR, and it is important to secure comprehensive rights to data because any processing activities regarding health data that does not comply with the purposes in art. 9.2 of GDPR will be unlawful. If explicit consent of the data subject is the legal basis for a lawful processing, the controller/processor shall ensure that the data subject has consented for the "*one or more specific purposes*" that they are interested in. As a general rule, and according to the purpose limitation principle under art. 5 of GDPR, personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".

Public interest sometimes overrides consent as a legal ground for health data processing in some instances, as explained in question 4.2. Key legal issues relating to personal data protection are outlined in question 4.3.

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 art. 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 abovementioned 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. Transfers of data directed to territories outside of the EEA seem very likely in the field of digital health services; the provider may need to obtain an authorisation or alternatively to prove that the country of destination has been subject to a decision of adequacy by the European Commission or to conduct a risk assessment and enter into Standard Contractual Clauses with the data importer.

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 art. 4.4 of Law 24/2015 of 24 July 2015 on patents (Spanish Patent Act), 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 AI and machine learning solutions *per se*, which are essentially software, i.e. a mathematical method, are not patentable. However, AI-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 formality, 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, art. 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 art. 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 patentable.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

The Spanish Organic Law 6/2001 on Universities regards technology transfer as one of the main functions of universities. This law also facilitates the involvement of professors in university spin-offs, e.g. temporary leaves of absence. In turn, the Spanish Law 14/2011 on Science, Technology and Innovation governs basic aspects of the technology transfer process, e.g., the application of private law to transactions between universities and companies.

Results of academic technology are generally transferred or licensed to third parties through invention assignments or licence agreements, respectively, or as a result of the creation of a spin-off company. Universities and Public research centres need to follow specific state regulations providing protection regarding the ownership of the creations, and are required to follow internal protocols that set out the terms for cooperation between university personnel and private entities. According to Law 14/2011, researchers shall in any case be entitled to share in the profits from the exploitation or assignment of their rights to such inventions obtained by the entities for which they provide their services.

On 30 March 2021, the Spanish Council of Ministers resolved to approve a preliminary draft law amending Law 14/2011 (https://ccoo.upv.es/files/Investigadores/2021/2021-04-01_AnteProyecto-Ley-modifica-Ley_14-2011_Ciencia-Tecnologia-Innovacion_BORRADOR_Ministerio-de-Ciencia-e-Innovacion.pdf). The draft regulates further incentives for academics to bring their research to market, or to create start-up companies building on research outcomes. In this sense, Communication 2014 C/198/01 of the European Commission provides guidelines for ensuring adequate compensation for public universities and public research organisations in their contracts with companies, which has a direct impact on the criteria for the preparation of budgets and intellectual and industrial property rights.

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).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

The Spanish Patent Act does not mention the condition that the inventor must be a natural person. However, the Guidelines published and followed by the Spanish Patent and Trademark Office for the examination of Spanish patent applications specifically establish that "*only natural persons can be designated as inventors, and never, legal persons*". Taking also into account that the understanding of the term inventor as referring to a natural person appears to be an internationally applicable standard, at this moment it is not possible for an AI device to be named as an inventor of a patent since the inventor must be a natural person in Spain.

The same is applicable at a European level. Although there is no express provision in the European Patent Convention (EPC) which states that the inventor must be a natural person, it recognises moral rights to the inventor and contains references to the inventor being a natural person. In that regard, in 2018 two patent applications in which the inventor was an AI system, referred to as DABUS, were filed before the European Patent Office (EPO). It rejected the application on the grounds that they do not meet the legal requirement of the EPC that an inventor designated in the application has to be a human being, and not a machine. The decision has been appealed before the Board of Appeal of the EPO.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

Government-funded inventions in Spain fall within the general regime for inventions, which includes the Spanish Patent Act, Royal Decree 316/2017 approving Regulations for the implementation of the Spanish Patent Act, and Orders ETU/296/2017 and ETU/320/2018. In addition, Royal Decree 55/2002 on the exploitation and transfer of inventions made in public research bodies sets, specifically, the ownership regime that must rule the inventions created by research staff working for several Spanish research agencies, such as the Spanish National Research Council and the Carlos III Health Institute.

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 healthcare and non-healthcare 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 healthcare 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 the 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, the data can be used for training purposes, and these should be referred.

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 the 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 the 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 artificial intelligence/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.

The correct allocation of IP rights under licensing contracts is also 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 solutions?

The 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 Union regarding AI. The European Parliament has adopted a Proposal for a Regulation on liability for the operation of AI systems, published on 20 October 2020. This proposal treats high-risk AI systems differently from other systems not considered so dangerous. Therefore, high-risk artificial intelligence systems operators are subject to a strict liability regime, albeit with very severe compensation limits; while systems that are not high risk are subject to a fault-based liability system, with reversal of burden of proof, and without specific compensation limits.

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. In the specific case of medical devices, Spanish Royal Decree 1591/2009 regulating medical devices rules that manufacturers who are not established within the European Union shall designate a single authorised representative within the European Union, both the manufacturer and the EU representative may be liable.

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 cyberattacks.

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

Regulation 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, when 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 healthcare 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.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Key barriers preventing widespread clinical adoption of digital health are not so much regulatory as they relate to organisational, budgetary or cultural reasons. The COVID-19 pandemic has been a turning point. The Digital Spain Plan 2025 identifies the following fields of action to increase the efficiency and quality of public healthcare services in Spain: (i) research to measure and improve health outcomes and to design preventive systems; (ii) support to patients in order to automatise and provide them with tools to be better informed in making health decisions; (iii) patient empowerment with telemedicine, self-diagnostic or enhanced accessibility tools; and (iv) streamlining of information systems to enable better data sharing and interoperability.

Leaving aside the prevailing attention to digitalisation of information, digital health solutions such as mHealth are not generally present in the clinical practice because they have not been generally incorporated in the public national health system and therefore are not financed.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Certification initiatives are mainly coming from the public sector rather than physician associations. We are not aware of any formal requirement of endorsement by physician certification bodies in Spain in order to introduce digital health solutions into clinical practice. Note, however, that some regional health authorities have accreditation and/or certification systems in place for mobile applications (mHealth). They award accreditations and/or include them in repositories of accredited apps for use in the regional public health system (Healthcare Quality Agency of Andalusia with the Distintivo AppSaludable (seal of quality) and Catalonia's TIC Salut Social and iSYS Score). Such accreditations are a driver for clinical adoption.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

There is no specific reimbursement process for digital health solutions within the Spanish health system. Spanish patients, when treated by the National Health System, receive all healthcare products and treatments included in the list of health benefits of the National Health System (Royal Decree 63/1995). Digital health solutions can be incorporated by the National Health System or by regional authorities, so that patients can benefit from them without charge. In this regard, each autonomous community may decide to incorporate digital health solutions that qualify as medical devices to their healthcare services. Regarding telemedicine, within the National Health System it is provided by the National Health System professionals and, therefore, does not need a reimbursement process.

Any medical consultations outside of the National Health System are not reimbursed, whether in person or via telemedicine, unless they are provided under an agreement between the services provider and the National Health System.

Montserrat Llopart is a Partner in the International Commercial & Trade department and leads the Healthcare and Compliance Law practises in the Baker McKenzie Barcelona office.
She is a regular speaker and contributor to specialist conferences and publications, and she is recognised by the leading legal directories such as *Chambers and Partners*, *The Legal 500* and *Best Lawyers* and in the *InspiraLaw* Top 50 Women's List for Spain and Portugal.
Montserrat is the former head of Baker McKenzie's Barcelona office and the Firm's pharmaceutical law group in the EMEA region.

Practice Focus

Montserrat assists healthcare companies throughout the lifecycle of healthcare products, from R&D to commercialisation and more specifically in the areas of clinical trials (agreements, regulatory procedures, processing of personal data), market access (pricing and reimbursement), products and companies regulations, commercial relations between healthcare industries (distribution, (co)promotion, manufacturing, supply, licensing, partnership agreements), relations with healthcare professionals and/or patients including compliance communication & advertising, e-health (connected devices, telemedicine, hosting of health data) and product liability. Her practice encompasses both advisory and litigation matters.

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

Sweden

Advokatfirma DLA Piper

Fredrika Allard

1 Digital Health

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 the World Health Organization (WHO), which is physical, psychological and social well-being.

1.2 What are the key emerging digital health technologies in your jurisdiction?

As a consequence of the COVID-19 pandemic, the use of digital healthcare meetings has increased rapidly, primarily within primary care. It is expected that use of digital healthcare meetings will continue to increase. Self-monitoring is also an area which is being established within several Swedish regions and which is predicted to have a breakthrough in the near future.

1.3 What are the core legal issues in digital health for your jurisdiction?

Secrecy and patient safety are core legal issues within digital health. Confidence in digitalisation within the healthcare sector is largely affected by how well sensitive data is protected.

1.4 What is the digital health market size for your jurisdiction?

There are no official numbers but according to a report issued by Inera on e-health and IT in the Swedish regions, the total costs for IT are expected to amount to SEK 14.04 billion for 2020, and purchases are expected to amount to approx. SEK 10.5 billion. Inera is a company owned by the Swedish regions, county councils and the SALAR.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

There is no publicly available list of companies in this broad sector. Coala Life, Visiba Care and Next Step Dynamics are, however, products which have been developed in Sweden and which have attracted much international attention in previous years.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The core healthcare regulatory schemes related to digital health are:

- 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 (HSLF-FS 2021:52).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Some of the other regulatory schemes that apply to digital health are:

- 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 healthcare devices or software in particular?

Other regulatory schemes that apply to consumer devices are the following:

- The Medical Device Regulation 2017/745 and supplementary regulations.

- The Product Safety Act (SFS 2004:451).
- The Product Liability Act (SFS 1992:18).
- Consumer Purchase Act (SFS 1990:932).
- E-commerce legislation such as the Distance and Doorstep Sales Act (2005:59).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? 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 and also assumes the responsibility for market surveillance related to medical devices. The MPA issues directives with the support of 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. *Integritetsskyddsmyndigheten*, IMY) 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?

The key areas of enforcement in digital health and healthcare 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.
- The Health and Social Care Inspectorate (IVO) supervises healthcare personnels' compliance with applicable healthcare legislation, such as the Patient Safety Act. IVO conducted an investigation on 13 digital healthcare providers in 2019 to ensure that patient safety is maintained when healthcare is performed at a distance.

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 EU Medical Device Regulation 2017/745 (MDR) which became applicable on 26 May 2021, unless the device benefits from the transitional provisions under the MDR. The MDR imposes, among other things, obligations on new actors such as distributors and importers. In order to be placed on the European market, the software must be CE-marked, which may, for certain classifications, require approval by a so-called notified body.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

There are no specific regulations regarding use of AI or machine learning. Products incorporating such technology will need to comply with general product legislation as applicable to the product in question. The European Commission has, however, proposed a regulatory framework on AI.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Integrity and data security issues, e.g. hackers' intrusion in networks and theft of personal data. All medical data regarding a patient must be kept confidential and leaks or losses of data may result in fines, damages and potential badwill.
- **Robotics**
  There are ongoing discussions regarding liability in relation to robotics. A core issue is foreseeing liability under mandatory legislation and proving the cause of damage.
- **Wearables**
  Integrity and data security issues, e.g. theft or loss of personal data, potentially sensitive personal data.
- **Virtual Assistants (e.g. Alexa)**
  See Telemedicine/Virtual Care and Wearables.
- **Mobile Apps**
  See Telemedicine/Virtual Care and Wearables.
- **Software as a Medical Device**
  Under the MDR (see question 2.6) more stringent rules apply. Most medical device software are furthermore up-classified under the MDR.
- **Clinical Decision Support Software**
  See Software as a Medical Device.
- **AI/ML powered digital health solutions**
  Risk of bias. 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. Issues relating to liability in terms of recommendations or advice given by AI is an ongoing debate and will most likely be important when algorithms assist in healthcare.
- **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 the use of internet of things (IoT) is almost always personal data, which means that specific rules apply, notably the GDPR.
- **3D Printing/Bioprinting**
  This technology is not well developed in Sweden, hence there are little or no guidelines regarding its use. Liability in terms of malfunctioning prosthetics or procedures

involving 3D-printed or bioprinted objects that lead to complications are issues that could arise. Legally classifying the printed object as either a medical product, biological product or, for example, a medical device may also be an issue which may become problematic in terms of CE-marking, for example. Furthermore, issues related to ethics, personal data and product safety are debated.

- **Digital Therapeutics**
  GDPR and more stringent rules imposed under the MDR.
- **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 without appropriate consent/permission.

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).

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). To the extent that data is handled by a public entity or organisation, the Public Access to Information and Secrecy Act (2009:400) may apply. 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 Data 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 as 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 the 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 the 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). The principles of personal data (e.g. purpose limitation, data

minimisation, etc.) under the GDPR also limits 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. 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. Following the judgment from the Court of Justice of the European Union, case C-311/18 (*Schrems II*), further safeguards may need to be taken, in addition to entering into such a data transfer agreement, depending on whether the recipient country's legislation or practices provides an essentially similar level of protection for the data as within the EU/EEA. The European Data Protection Board has issued recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

It is essential that any data that is used or collected, especially concerning personal and/or patient data, complies with the GDPR and other national laws and regulations relating to patient data. Data used or collected illicitly, wrongfully or on improper grounds may result in hefty fines and bad will towards the company.

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 (the data exporter is responsible) and for the subsequent use by the data importer (the data importer is responsible).

Please see above regarding the 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, but may also need to include further safeguards, see question 4.5.

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

Please see the 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 the 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, however, not regarded as "employees" under the act, and the rights to patentable inventions therefore remain with the individual.

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 rules or laws that apply to academic technology transfers in your jurisdiction?

As mentioned under question 6.1, teachers are exempted from the definition of "employees" under the Right to the Inventions of Employees Act why the general rule that the employer owns patentable inventions that arise as a result of an employee's activities or within the employment context does not apply to teachers. The exclusive rights to patentable inventions hence remain with the inventor, leaving him/her the right to, for example, commercialise the rights, unless otherwise agreed. Many educational institutions apply the teacher's exemption also to other intellectual property rights than patents.

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.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

No. The inventor must have legal capacity. AI does not currently have legal capacity under Swedish law.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

See question 6.1 and 6.4 above.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

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 healthcare and non-healthcare 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 licence 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 solutions?

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 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.

10 General

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

Compliance with data protection legislation is a key issue. Further, several Swedish healthcare providers are subject to the Public Access to Information and Secrecy Act (2009:400), according to which, information which is subject to secrecy may not be disclosed. Swedish regions are therefore reluctant to engage service providers which use cloud-based services where the server is placed in the U.S. due to the U.S. legislation the Cloud Act, as, in short, entities may be required to disclose information on its servers to U.S. authorities. Many regions therefore choose service providers where data is stored in the EU/EEA.

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-healthcare companies should consider before entering today's digital healthcare market?

Sweden is a tech-savvy nation with the majority of the population having access to the 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. Further, it is important to understand how one's product fits into the ecosystem of the healthcare providers in Sweden.

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

Implementing the right incentives in order to ensure that management remains with the company after the take-over in order to not lose valuable knowledge and expertise.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

A key barrier is unclarity in legislation leading to different interpretations within the regions (i.e., the buyers of digital solutions). Another key barrier is the trust in digital health solutions regarding the security of keeping personal/patient data confidential and GDPR, which has become increasingly important. The additional cost of educating and instructing healthcare personnel in new digital solutions is another barrier.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

All of Sweden's regions collaborate to achieve an equal, cost-effective and appropriate use of new medical devices throughout Sweden through the nationally managed introduction. The Medical Technology Product Council (Sw. *MTP-Rådet*) determines which medical devices, which may include software, are suitable for national collaboration and provides recommendations on how they should be introduced and used.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Medical devices, such as digital health solutions for self-monitoring, may be subsidised by the state upon application to the Dental and Pharmaceutical Benefits Agency, TLV, by the manufacturer. The TLV determines whether the product shall be part of the Swedish benefits scheme and determines the price for the product.

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 LIF trade association.
Fredrika also works with different types of IT and commercial agreements, consultancy and cooperation agreements in various sectors.

Advokatfirma DLA Piper
Sveavägen 4, Box 7315
SE-10390 Stockholm
Sweden

Tel: +46 704 808 115
Email: fredrika.allard@se.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

Switzerland

Dr. Stefan Kohler

Christian Wyss

VISCHER AG

1 Digital Health

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 digital health technologies in your jurisdiction?

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 digital health for your jurisdiction?

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 current 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.

1.4 What is the digital health market size for your jurisdiction?

The potential for digitisation of the healthcare system in Switzerland is seen primarily in addressing rising healthcare spending. Studies conclude that full implementation of digitisation opportunities available today could save up to CHF 8.2 billion or around 12% of Switzerland's total healthcare costs (McKinsey Digital; Digitization in healthcare: The CHF 8.2 billion opportunity for Switzerland, September 2021).

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

Currently, no information is publicly available on the most successful digital health companies in Switzerland. This is not surprising, as this innovation is largely driven by privately held start-ups. These start-ups typically offer their achievements in cooperation with established health insurance companies, hospitals, pharmaceutical and medtech companies, and other established companies in the healthcare sector.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Please note the following core healthcare regulatory schemes relating to digital health in Switzerland:

- 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).
- 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 core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The Swiss Parliament passed the new data protection law in the fall of 2021. It is expected that the new law will come into force in the second half of 2022.

In addition to the transparency and integrity rules of the Therapeutics Products Act, the Act against Unfair Competition (no. 241), which penalises both active and passive corruption, is relevant for corruption offences.

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.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

In Switzerland, digitised applications (including software) that fulfill a medical purpose are regulated by the Medical Devices Ordinance (MedDO), revised as of May 26, 2021. Although the European Union no longer recognises Swiss medical device law as equivalent as of May 26, 2021, the revised Swiss MedDO adopts the provisions of European regulation, in particular the MDR, with regard to the regulatory requirements of medical devices, including those in the area of digital health. Conformity assessments of digitised applications in the medical device sector in the EU are (unilaterally) recognised by Switzerland.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

Please note the following regulatory authorities relating to digital health in Switzerland:

- **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.

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

Some of the key areas of enforcement relating to digital health are as follows:

- 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 or Conformity Assessment Bodies in the countries concerned.

2.7 What regulations apply to Artificial Intelligence/Machine Learning powered digital health devices or software solutions and their approval for clinical use?

Artificial Intelligence/Machine Learning devices or software that serve a medical purpose directed at an individual are considered Medical Devices under the MedDO. They may only be placed on the market if a declaration of conformity is available for them. As part of this conformity assessment, a risk analysis is carried out to determine whether the device or software, when used as intended, does not endanger the health of users, consumers, patients or third parties.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - Depending on their characteristics, telemedicine or virtual care 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).
  - Telemedicine or virtual care 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. Some cantonal legislations treat telemedicine or virtual care restrictively because they require the physician to physically meet and treat the patient.
  - The health data transferred via telemedicine or virtual care 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 telemedicine or virtual care platforms. Medical due diligence must be ensured at all times. According to the case law of the Swiss Federal Supreme Court, prescribing medicines via telemedicine or virtual care platforms requires that the patient receives personal and serious advice from a doctor. Some cantonal legislations treat telemedicine or virtual care restrictively because they require the physician to physically meet and treat the patient.
  - 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, healthcare 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 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.
- **Clinical Decision Support Software**
  Clinical Decision Support Software usually serves a medical purpose focused on an individual and would then be classified as a medical device. The MedDO would then be applicable to them. Such clinical decision support software may only be placed on the market if a declaration of conformity is available for it.
- **AI/ML powered digital health solutions**
  A conformity assessment under the MedDO is required for placing AI/ML powered digital health solutions on the market, if a medical purpose directed at an individual can be ascribed to them (*cf.* question 2.7 above). Conformity can only be confirmed if it can be established that the health of users, consumers, patients or third parties is not endangered when used as intended.
- **IoT and Connected Devices**
  - If the Internet of Things (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.
- **3D Printing/Bioprinting**
  - Suppliers of the CAD files required for 3D printing must consider whether their print commands are subject to copyright protection. The external design of 3D printed products may be subject to third-party trademark or design protection, and their technical functionality may be subject to third-party patent protection.
  - The question of who is liable in the event of damage from defective 3D printing products can be complex and should be clarified in advance.
- **Digital Therapeutics**
  Digital therapies or therapy aids are to be classified as medical devices if a medical purpose directed at an individual can be ascribed to them. The MedDO would then be applicable to them. Such digital therapies or therapy aids may only be placed on the market if a declaration of conformity is available for them.
- **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 publicly listed hospitals but also privately 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 Arts 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 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 or 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 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.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

In Switzerland, there is no specific law on the issue of data entitlement. If data collections are involved, they can qualify as copyright works to which the author can claim ownership. For the rest, however, data are basically to be qualified as know-how for which no special legal protection exists. However, the provisions on the protection of trade and manufacturing secrets, in particular in the Act against Unfair Competition and the Criminal Code, remain reserved.

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 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 Revised 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 rules or laws that apply to academic technology transfers in your jurisdiction?

On a federal level, academic technology transfer is governed by the Federal Act on the Federal Institutes of Technology (ETH Act) and in particular by the Ordinance of the ETH-Council regarding intellectual property rights in the ETH area. On a cantonal level, academic technology transfers are governed by the cantonal laws applying to the Universities. Most public research and educational institutions and university hospitals (PROs) in Switzerland have professionally organised bodies that ensure technology transfer with the private sector.

The Swiss Technology Transfer Association (swiTT) reunites these bodies responsible for technology transfer both on the federal and cantonal levels and fosters the following main principles:

- Partnership: The cooperation between private enterprises 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, 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 the 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).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

Based on articles 3 and 5 of the Federal Act on Patents for Inventions (Patents Act), only individuals can be inventors of a patent. Thus, an artificial intelligence device cannot be named as an inventor of a patent in Switzerland. However, the Swiss Federal Institute of Intellectual Property (IPI) is actively participating in the WIPO dialogue on intellectual property and artificial intelligence, which includes the question of whether a human being should be named as the inventor or whether it should be permitted to name an AI application as the inventor of an AI-generated invention. It is expected that both the IPI and the Swiss legislator will follow these discussions and suggest appropriate amendments to the Patents Act should the WIPO dialogue reveal that allowing artificial intelligence devices to be named as an inventor of a patent constitutes an important element to facilitate and exploit AI-based innovation.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The main rules for inventions funded by the Swiss federal government are stated in the Federal Act on the Promotion of Research and Innovation (RIPA). Article 27 RIPA governs the exploitation of research findings funded pursuant to the RIPA, which is further clarified in articles 40 and 41 of the Ordinance to the Federal Act on the Promotion of Research and Innovation.

Important details about innovation project funding are laid down in the Ordinance of the Swiss Innovation Promotion Agency on its Funding and Other Support Measures (Innosuisse Funding Ordinance). Innosuisse together with the academic research partners and the industry implementations partners profit from a wide discretion on how to allocate intellectual property rights arising from Innosuisse-funded research and on which terms they may be used and exploited by the industry implementation partners.

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 healthcare and non-healthcare 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.

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 licences 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 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 solutions?

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. Arts 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 Arts 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 Swiss law is applicable according to Art. 133 para. 1 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 for 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 another 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-healthcare companies should consider before entering today's digital healthcare 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 healthcare 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.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

A key barrier for widespread clinical adoption is switching the financing of digital health solutions from project-based financing to a sustainable financing through hospitals' ordinary budgets, health insurance providers, and patients. While it is relatively easy to get initial financing via research grants, industry collaborations, foundations, innovation budgets or similar sources, the switch to sustainably financing the costs of digital health solutions is a real challenge. Healthcare financing is not only controlled by market forces, but – to a large extent – by both federal and cantonal politics. Financing schemes and incentives differ substantially between publicly owned and privately owned hospitals, between hospitals and outpatient healthcare facilities, and – to a lesser extent – between big university hospitals and smaller hospitals without academic affiliation. Unlocking the full potential of many digital health solutions, however, often requires not just a few, but a majority of players adopting a particular solution.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Switzerland, such clinical certification bodies are not known. However, Swiss regulation is strongly oriented towards the European Community. Therefore, the bodies relevant there are also indirectly relevant for regulation in Switzerland.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Reimbursement under the Swiss health insurance law for outpatient treatments or therapies is in principle also available to

digital health solutions. However, reimbursability requires that this is expressly provided for by the applicable regulations or is recognised by the health insurers within the framework of tariff agreements. In order for reimbursement to be obtained, a formal process must be completed with the appropriate health authority or health insurance provider.

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 enabled 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 programme 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: kohler@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
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: Basel; Geneva; and Zurich. 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

Taiwan


Hsiu-Ru Chien


Eddie Hsiung


Shih-I Wu

Lee and Li, Attorneys-at-Law

1 Digital Health

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

There is no clear definition of "digital health" under Taiwan law. In general, "digital health" should cover areas such as mobile medicine (mHealth), medical health information (Health IT), wearable devices, telehealth and telemedicine, personalised medicine, and other applications of information and communication technology (ICT) in the medical and health fields.

1.2 What are the key emerging digital health technologies in your jurisdiction?

Based on Taiwan's complete semiconductor and ICT industry supply chain, cross-border integration of medical technologies, as well as innovative digital health technologies such as healthcare big data, Internet of Things (IoT), artificial intelligence (AI) and 5G technology, biomedical chip technology, sensors, wearable devices, biobank, telehealth and telemedicine are being invested, created and developed in various fields and industries, and also by government organisations.

1.3 What are the core legal issues in digital health for your jurisdiction?

With respect to digital health in the context of a medical device, it is subject to regulations under the Medical Devices Act, which took effect on May 1, 2021. The term "medical device", as defined in the Medical Devices Act, shall refer to instruments, machines, apparatuses, materials, software, reagents for *in vitro* use, and related articles thereof, whose design and use achieve one of the following primary intended actions in or on the human body by other than pharmacological, immunological, metabolic, or chemical means: (a) diagnosis, treatment, alleviation, or direct prevention of human diseases; (b) modification or improvement of the structure and function of human body; and (c) control of conception.

From a Taiwan legal perspective, the manufacturing or importation of medical devices may be conducted only after a medical device permit licence that grants registration and market approval is issued by the government authority.

Personal data protection is also a critical issue where any personal data is to be collected, used, or processed in the course of providing any digital health products or services.

1.4 What is the digital health market size for your jurisdiction?

There are no official statistics concerning the digital health market size in Taiwan. Nonetheless, according to the estimated data of the Industrial Technology Research Institute, Taiwan's precision health market was estimated to be about NT$8.75 billion (around US$300 million) in 2020 and to reach NT$14.2 billion (around US$490 million) in 2025, with a compound annual growth rate of 10.2%; the growth rates for digital health, precision medicine, and regenerative and immunomedicine composites were estimated to be about 11%, 11.5%, and 4.8%, respectively.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

In Taiwan, the digital health market is mostly invested in by major electronic technology companies. The revenue of these companies is calculated on the basis of the overall enterprise, so it is difficult to distinguish their revenue or rank with respect to the digital health field.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The Medical Devices Act provides for core regulations governing medical devices.

As indicated under question 1.3, the manufacturing or importation of medical devices is only allowed after a medical device permit licence that grants registration and market approval is issued by the Ministry of Health and Welfare (MOHW).

Medical device manufacturing must comply with the guidelines set forth in the Good Manufacturing Practice (GMP) under the Pharmaceutical Good Manufacturing Practice Regulations.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Depending on the issues involved, the following laws and their related regulations apply:

- The Personal Data Protection Act.
- The Physicians Act.
- The Consumer Protection Act.
- The Civil Code.
- The Telecommunications Act.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The Consumer Protection Act and the Civil Code are the main laws providing for the relevant consumer rights and product liabilities. The manufacturing and sale of consumer devices should also follow the regulations under the Commodity Labelling Act and the Commodity Inspection Act.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The MOHW is the competent authority responsible for supervising healthcare-related matters, products and industries. The MOHW has a broad mandate to improve the quality of healthcare.

Under the MOHW, the Food and Drug Administration (TFDA) is responsible for regulating the system for the safety and quality of food, drugs, medical devices, and cosmetics. The TFDA grants product registration and clinical trial approvals, monitors manufacturing and importation, and conducts safety surveillance activities on health-related products.

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

The Medical Devices Act outlines a three-tier risk-based classification system for medical devices: Class I products with low risk; Class II products with medium risk; and Class III products with high risk.

Additionally, any person who manufactures or imports medical devices without the required prior approval may be subject to imprisonment for not more than three years and may, in addition thereto, be imposed with an administrative fine of not more than NT$10,000,000.

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

In addition to the regulations mentioned in our answer to question 2.1, the Guidance for Medical Software Classification as announced by the TFDA also applies to Software as a Medical Device. On December 24, 2020, the TFDA announced the revision of the Guidance for Medical Software Classification, which excludes medical software used to measure heart rate and blood oxygen (including wearables) for daily health management of the general public within the scope of a medical device, if they are not related to the diagnosis or treatment of diseases. Recognition of classification is still subject to the judgment of the competent authorities.

2.7 What regulations apply to Artificial Intelligence/Machine Learning powered digital health devices or software solutions and their approval for clinical use?

No specific regulations are enacted specifically for AI/Machine Learning (ML) powered digital health devices or software solutions. Medical devices are all governed by the Medical Devices Act; Chapter IV of the Medical Devices Act provides for regulations concerning management of medical device clinical trials.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - Service provider – Pursuant to the Physicians Act, a physician may not treat, issue a prescription or certify a diagnosis to patients that are not diagnosed by the physician himself or herself except for certain special (i.e., remote areas) or urgent circumstances. Therefore, physicians are not allowed to provide telemedicine services under current laws in general.
  - Regulations for medical devices – The regulations mentioned in our answer to question 2.1 should be complied with if the equipment/devices involved are considered as medical devices.
  - Personal data protection – Taiwan's personal data protection law should also be followed if any personal data is to be collected, used, or processed.
  - Product liability – Manufacturers and sellers of products are subject to the duties and liabilities under the Consumer Protection Act and the Civil Code.
  - Attribution of responsibility – Provision of the service of telemedicine may involve the user (patient), the healthcare service provider (physician) and the manufacturer/seller of the product. The attribution of responsibility of the relevant parties should be determined generally based on the contracts as well as the tort law (Civil Code and Consumer Protection Act).
- **Robotics**
  Similar issues as for Telemedicine/Virtual Care regarding regulations for medical devices, personal data protection, product liability, and attribution of responsibility.
- **Wearables**
  Similar issues as for Telemedicine/Virtual Care regarding regulations for medical devices, personal data protection, and product liability.
- **Virtual Assistants (e.g. Alexa)**
  Similar issues as for Wearables.
- **Mobile Apps**
  Similar issues as for Wearables.
- **Software as a Medical Device**
  Similar issues as for Wearables.
- **Clinical Decision Support Software**
  Similar issues as for Robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **AI/ML powered digital health solutions**
  Similar issues as for Robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **IoT and Connected Devices**
  Similar issues as for Wearables.

- **3D Printing/Bioprinting**
  Similar issues as for Wearables.
- **Digital Therapeutics**
  Similar issues as for Robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **Natural Language Processing**
  No special regulations for Natural Language Processing.

3.2 What are the key issues for digital platform providers?

The Personal Data Protection Act is the main law governing the collection, processing and use of personal data so as to prevent harm to personality rights, and to facilitate the proper use of personal data. Digital platform providers should follow the requirements under this Act if any personal data is involved in the products or services provided by digital platform providers.

4 Data Use

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

Under Taiwan law, the Personal Data Protection Act (PDPA) is the main law governing personal data protection. The key issues to consider for use of personal data under the PDPA include, among others, the following:

- Whether the data is considered "personal data" under the PDPA.
- Whether the "personal data" is considered "sensitive personal data" under the PDPA. Please see our response to question 4.4 for the definition of "sensitive personal data".
- Whether the use of personal data complies with relevant requirements under the PDPA, such as the requirement to obtain the necessary informed consent from the data subject as required by the PDPA, etc. (or whether any exemption from the requirement applies).

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

The considerations indicated in our response to question 4.1 above would not change regardless of the nature of the entities involved; however, the available types of exemptions from the requirement to obtain informed consent from the data subject are different between non-government entities and government entities.

4.3 Which key regulatory requirements apply?

Under the PDPA, unless otherwise specified by law, a company is generally required to give notice to (notice requirement) and obtain consent from (consent requirement) an individual before collecting, processing or using any of said individual's personal information (i.e., the "informed consent" requirement), subject to certain exemptions. To satisfy the notice requirement, certain matters must be communicated to the individual, such as the purposes for which his or her data is collected, the type of the personal data and the term, area and persons authorised to use the data, etc.

In case the personal data is regarded as "sensitive personal data" (please see our response to question 4.4), the consent must be made in writing, and the following must be complied with: (i) the collection, processing or use must not exceed the necessary scope of the specific purpose(s); (ii) the collection, processing or use based solely on the consent of the data subject is not otherwise prohibited by law; and (iii) such consent is not given by the data subject out of his/her free will.

4.4 Do the regulations define the scope of data use?

Pursuant to the PDPA, "personal data" is defined broadly to include: name; date of birth; I.D. card number; passport number; characteristics; fingerprints; marital status; family information; education; occupation; medical record, medical treatment and health examination information; genetic information; sexual life information; criminal record; contact information; financial conditions; social activities; and other information which may directly or indirectly identify an individual. Additionally, personal data pertaining to a natural person's medical records, healthcare, genetics, sex life, physical examination, and criminal records are known as "sensitive personal data", and thus generally subject to stricter regulations under the PDPA.

4.5 What are the key contractual considerations?

In case any collection, use, or processing of personal data is contemplated under a contract, it is suggested that the above-mentioned "informed consent" requirement be fully complied with, unless any of the available exemptions are satisfied. Additionally, it may be arranged to have the parties (or, at least for the party who will actually collect, use, or process personal data) agree to the "compliance clause" to ensure a party's compliance with the PDPA throughout the contract period.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Compliance with the PDPA, in particular, obtaining required "informed consent" for collection, use and processing of personal data and using and processing the collected personal data within the necessary scope of the specific purpose(s), is the key legal issue as any violation of the PDPA (e.g., unlawful collection, use or processing of personal data) may be subject to civil, criminal, and/or administrative liabilities. For example:

- Civil liability: A company would be liable for the damages caused by any unlawful collection, processing, or use of personal data due to its violation of the PDPA (Article 29 of the PDPA).
- Criminal liability: Any unlawful collection, processing, or use of personal data in violation of the PDPA with the intention of obtaining unlawful gains and thereby causing damage to others would be subject to imprisonment for no more than five years and may, in addition thereto, be imposed with a criminal fine of not more than NT$1,000,000 (Article 41 of the PDPA).
- Administrative liability: Any unlawful collection, processing, or use of personal data in violation of the PDPA may be required to be corrected, and any failure to correct such violation within a specified period of time would be subject to an administrative fine (Articles 47 and 58).

5 Data Sharing

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

Please see our response to question 4.1 above, as sharing personal data would be considered to fall within the definition of "processing" and/or "use" of personal data under the PDPA.

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

Please see our response to question 4.2 above.

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

Please see our response to question 4.3 above.

Please also note that, in case the personal data is regarded as "sensitive personal data" (please see our response to question 4.4), an exemption from the "informed consent" requirement for collection, use and processing of personal data (including data sharing) is "where it is necessary for statistics gathering or academic research by a government entity or an academic institution for the purpose of healthcare, public health, or crime prevention, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject".

6 Intellectual Property

6.1 What is the scope of patent protection?

According to the Patent Act, the subject of a patent right may be an invention, a utility model, or a design:

- Invention – the creation of technical ideas, utilising the laws of nature.
- Utility model – the creation of technical ideas relating to the shape or structure of an article or combination of articles, utilising the laws of nature.
- Design – the creation made in respect of the shape, pattern, colour, or any combination thereof, of an article as a whole or in part by visual appeal. For computer generated icons (Icons) and graphic user interface (GUI) applied to an article, an application may also be filed for obtaining a design patent.

Under the Patent Act, any invention/utility model/design is patentable provided it complies with the requirements for patentability, such as novelty, inventive step and enablement. However, please note that diagnostic, therapeutic and surgical methods for the treatment of humans shall not be granted a patent under the Patent Act. Thus, if a concerned "digital health" invention or technology involves diagnostic, therapeutic and surgical methods for the treatment of humans, it may be deemed an unpatentable subject matter.

Moreover, a digital health invention or technology may relate to the creation of a software or an algorithm. "The Examination Guidelines for Computer-related Inventions" provide rules for deciding whether such invention can be granted a patent. The Guidelines classify statutory subject matters for software patents: process; product; and computer-readable storage media. "Process" is defined as a series of specific operational steps to be performed on or with the aid of a computer. "Product" encompasses a computer or other programmable apparatus whose actions are directed by a computer program or another form of software. "A computer-readable storage medium" is an article of manufacture that, when used with a computer, directs the computer to perform a particular function. Software patents are patentable if the data format interacts with computer software or hardware to produce technical effects (such as enhancing data processing, storage performance, security, etc.).

6.2 What is the scope of copyright protection?

A "work" under the Copyright Act means a creation that is within a literary, scientific, artistic, or other intellectual domain, which includes oral and literary works, musical works, dramatic and choreographic works, artistic works, photographic works, pictorial and graphical works, audio-visual works, sound recordings, architectural works, and computer programs. There are no registration or filing requirements for a copyright; however, there are certain features that qualify for being copyrighted, such as "originality" and "expression".

Software designed for "digital health" can be protected through copyright.

6.3 What is the scope of trade secret protection?

Trade secrets are protected if they satisfy the following constituent elements: information that may be used in the course of production, sales or operations; has the nature of secrecy; has economic value; and its owner has taken reasonable measures to protect the secrecy. There are no registration or filing requirements for a trade secret to be protected by law.

To keep trade secrets confidential during court proceedings, the court trial may be held in private if the court deems it appropriate or it is otherwise agreed upon by the parties. In an intellectual property-related lawsuit, the parties may apply to the court to issue a "protective order", and the person subject to such protective order should not use the trade secrets for purposes other than those related to the court trial and should not disclose the trade secrets to those who are not subject to the order.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

In general, academic institutions have specific internal policies to regulate the ownership and management of the technologies created by their scholars, researchers, graduate students, and employees. Academic institutions may license or assign their IPs to a third party for commercial purposes.

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

Software can be protected by intellectual property rights such as patents, copyrights or trade secrets. For software-implemented inventions such as a medical device, if it coordinates software and hardware to process information, and there is a technical effect in its operation, it might become patentable.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

In judicial practice, an artificial intelligence device cannot be named as an inventor of a patent. Judgments from the Taiwan Intellectual Property and Commercial Court hold that a patent invention is the creative output of the human spirit, and cannot be created by an artificial intelligence device; from the perspective of Taiwan laws, only natural or legal persons can enjoy such rights.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

For projects in scientific and technological research and development to be subsidised, commissioned, or funded by the government, or to be conducted under scientific and technological research and development budgets prepared by public research institutions (organisations) pursuant to law, the "management and utilisation of the R&D results" should comply with the Fundamental Science and Technology Act and the Government Scientific and Technological Research and Development Results Ownership and Utilisation Regulations. Specifically:

- The R&D results and the income from such a project may be conferred, in whole or in part, to the executing R&D units for ownership or licensing for use, and are not subject to the National Property Act.
- The ownership and utilisation of the R&D results and the income therefrom should be determined based on the principles of fairness and effectiveness by assessing the percentage contribution of capital and labour, the nature of the R&D results, potential uses, societal benefits, national security, and impact on the market.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Issues in relation to the rights (especially the IP ownership), obligations and division of responsibilities are critical for collaborative improvements. The applicable laws and agreements between the parties would need to be carefully analysed and arranged for in this regard.

For a collaborative improvement involving a fund provider and an inventor/developer, the IP laws adopt similar rules to govern the ownership of the said improvement. With respect to patent rights and trade secrets, the agreement between the parties shall prevail, or such rights will be vested in the inventor or developer in the absence of such agreement, and the fund provider may use such invention.

With respect to copyright, the person who actually creates the work is the author of the work unless otherwise agreed upon by the parties; the economic rights arising from the work should be agreed upon by the parties, or the author owns such rights in the absence of such agreement. However, the commissioning party (fund provider) may use the work.

For improvements that are jointly made by several parties, attention shall be paid to the issue of co-ownership. The Patent Act clearly provides the following provisions for co-owned patents:

- Where a right to apply for a patent is jointly owned, the patent application related thereto shall be filed by all the joint owner(s). If a co-owner contravenes the provision for "joint-application" by individually filing an application and obtains a patent as a result thereof, other co-owners may file a cancellation action with respect to such patent and seek revocation of the patent right.
- Where the right to apply for a patent is jointly owned, the right to apply for the patent shall not be assigned or abandoned without the consent of all joint owners. Where the right to apply for a patent is jointly owned by two or more persons, none of the joint owners shall assign his/her own share therein to a third party without the consent of other joint owners. Where one of the owners of the right to apply for a patent abandons his/her own share, this share shall be vested in other joint owner(s).
- Where a patent right is jointly owned, except for exploitation by each of the joint owners, it shall not be assigned, entrusted, licensed, pledged, or abandoned without the consent of all the joint owner(s). Where a patent right is jointly owned, no joint owner may assign, entrust or establish a pledge on his/her own share without the consent of all the other joint owner(s). Where a joint owner of a patent right has abandoned his/her own share, this share shall be vested in other joint owner(s).

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

As indicated in our answer to question 2.1 above, the manufacturing or importation of medical devices is only allowed after a medical device permit licence granting registration and market approval is issued. Given that, whether the company has or is required to obtain the permit licence would be a critical issue.

8 AI and Machine Learning

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

According to our understanding of the practice, the current applications of machine learning include, among others: (i) clinical decision support: for example, analysing medical images with machine learning to improve the accuracy of diagnosis results; and (ii) big data forecasting: by analysing large amounts of data, tracking or forecasting the relationships between different medicines and side effects.

Please note, however, that although an AI might be able to make decisions by itself, under current Taiwan law, only a licensed physician may practice as a physician. Thus, AI and machine learning are merely "technologies" or "tools" to assist physicians.

8.2 How is training data licensed?

If any personal data would be collected, used or processed with respect to training data/data licensing, the PDPA regulatory regime (e.g., our response to sections 4 and 5) would apply – for example, it should be arranged to have the data collector obtain the necessary "informed consent" unless any exemption applies. If any intellectual property is involved in the licensing, it is suggested that the customary licensing practice (e.g., IP licensing agreement to be entered into by the licensor and licensee) be followed.

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

Determining the owner of the intellectual property of an AI-created work is expected to be a legal issue that will be widely discussed as AI use develops and becomes more widespread. According to the views of many experts and scholars, AI development can be generally divided into the following three phases, and we are currently in phase 2:

(i) Phase 1: all intrinsic knowledge/information of AI is given by humans, and AI simply functions as a tool to respond to human query inputs. AI does not have the ability to learn or think.

(ii) Phase 2: AI learns through computer software designed by humans, which is called "deep learning". In addition to responding to human query inputs, AI is able to use its limited intrinsic perception and logic to help its users make decisions.

(iii) Phase 3: AI has evolved to have the ability to think for itself and act sufficiently like a human (i.e., it may have perceptions and emotions). That is, AI has a self-training ability, and the ability to evaluate, determine, and solve problems.

With respect to phase 1, as the AI merely functions as a tool utilised by humans to create a work or invention, the human (user of the AI) should be the owner of the intellectual property (copyright or patent).

In phase 2, AI already has the ability of deep learning, and it is not merely a tool for humans. However, there would be issues as to whether AI has the ability to create an "original expression" under copyright law or to be an "inventor" under patent law, and if not, whether the human using the AI can be considered as the one who actually creates the "expression" or the invention. Such issues would be more important and cannot be ignored in phase 3, when AI has evolved to have the ability of independent thinking and can create an "expression" and make an invention like a human.

We believe that the above view is also generally supported by a letter of interpretation issued by Taiwan's Intellectual Property Office (IPO) dated April 20, 2018 (Ref. No.: 1070420), which provides that as AI is not a "person" from a legal perspective, any AI-created work cannot be protected by copyright.

In general, our preliminary view is that such issues might not be solved under the current IP regime in Taiwan; it is a real challenge faced by, and needs to be addressed by, the government, legislators, representatives of the court system, and other legal practitioners in the future along with the development of AI.

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

As indicated in our response to question 8.2, if any "personal data" would be collected, used or processed with respect to training data/data licensing, the PDPA regulatory regime (e.g., our responses to sections 4 and 5) would apply. Specifically, in case of any "sensitive personal data", more restrictions would apply – such as the requirement that the "informed consent" be in writing (see question 4.3). We believe PDPA compliance as indicated should be carefully considered with respect to data licensing.

9 Liability

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

The theories of liability applying to adverse outcomes are mainly as follows:

- Civil liability – breach of contract, torts and product liability: the Civil Code; and the Consumer Protection Act would apply.
- Criminal liability – injury (intentional act or negligence) or carrying out activities of manufacturing or importation without required permit or approval: the Criminal Code; the Physicians Act; and the Medical Devices Act would apply.
- Administrative liability – carrying out activities of manufacturing or importation without required permit or approval; the Medical Devices Act would apply.

9.2 What cross-border considerations are there?

In case any digital health-related services are provided to Taiwan persons from offshore, there might be an issue as to whether such offshore entity would be required to comply with the Taiwan regulatory requirements regarding licensing (e.g., prior approval/permit/licence required for running a medical device company or carrying out healthcare-related activities) as healthcare is a regulated industry in Taiwan. Please also see our response to question 10.2 for such regulatory requirements.

From a contract perspective, even if the governing law of the contract for the digital health-related service is foreign law (i.e., non-Taiwan law) and a foreign court is agreed in the contract for dispute resolution, we still cannot completely rule out the possibility that in case of any dispute where the Taiwan customers file the suit in a Taiwan court, the Taiwan court would still review the matter and rule that the Taiwan laws (such as the Taiwan Consumer Protection Act) would apply in order to protect said Taiwanese persons.

10 General

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

With respect to cloud-based services for digital health, the PDPA will be applicable, as an organisation using the cloud-based service may carry out the activities of collecting data from the data subjects, which would then be passed to a service provider for processing and use. Therefore, from a Taiwan legal viewpoint, the key issue in cloud-based services for digital health is PDPA compliance. Please see our responses to sections 4 and 5, specifically, where personal data is considered "sensitive personal data", the requirement for the informed consent be in writing (see question 4.3), and an exemption from the "informed consent" requirement for use by non-government entities or academic institutions under certain circumstances (see question 5.3).

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

Please note that healthcare is a regulated industry in Taiwan. For example, running a medical device company, as well as manufacturing and sale of medical devices, would require prior approval/permits under current regulations. Additionally, pursuant to the Physicians Act, a person may not practice medicine as a physician without a required licence, and, in the context of telemedicine, a physician may not treat, issue a prescription or certify a diagnosis to patients that are not diagnosed by the physician himself or herself except for certain special (i.e., remote areas) or urgent circumstances (please also see question 3.1 above).

Given the above, it is advisable for non-healthcare companies to consider the above licensing/regulatory requirements before entering the digital healthcare market in Taiwan.

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

From a legal perspective, it is suggested that venture capital and private equity firms analyse in depth whether the target digital healthcare venture's business model is in line with Taiwan's regulatory regime at the due diligence stage – most importantly, the compliance with licensing/regulatory requirements as indicated under question 10.2 above as well as the PDPA compliance, especially if the personal data collected by the target company would involve "sensitive personal data".

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

According to our observation, the current legal obstacles in Taiwan that would hinder the developments of digital health solutions may include, for example: (i) as indicated in question 3.1, a physician may not treat, issue a prescription or certify a diagnosis to patients that are not diagnosed by the physician himself or herself except for certain special (i.e., remote areas) or urgent circumstances. Therefore, providing telemedicine services by physicians are generally not permitted under current laws in Taiwan; or (ii) there are generally more restrictions on collection, use and processing of "sensitive personal data", which should be normally involved as to development of digital health solutions.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Taiwan, physician certification bodies (e.g., Taiwan Surgical Association,) do not play an important role in the clinical adoption of digital health solutions. Compliance with existing regulatory requirements is of the most importance. Please see our response to question 10.2 above for the licensing/regulatory requirements that need to be followed from a Taiwan regulatory perspective.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

To our knowledge, there are no private insurers that specifically exclude patients who utilise digital health solutions from filing insurance claims when an insured matter occurs and no additional documentation is required, unless it is specified in the insurance policy. Regarding the reimbursement by the government, we notice that there is a pilot plan announced by the National Health Insurance Administration in 2020 aiming to include virtual care for remote areas in the coverage of our National Health Insurance. Under the said pilot plan, patients who are seen through medical institutions approved to conduct virtual care may only need to pay for registration fees, subject to certain exceptions specified in relevant regulations.

Hsiu-Ru Chien has educational backgrounds in science, management and law, and is a certified attorney-at-law and patent attorney in Taiwan. She also passed the Chinese Patent Bar in 2013. Her practice focuses on patent prosecution, enforcement, licensing and transactions as well as other IP-related matters. She is serving as the Deputy Secretary of General of the Taiwan Patent Attorney Association. As a partner of Lee and Li, she periodically publishes IP-related articles in international journals such as the *World Intellectual Property Report* and *International Law Office Newsletter*. She has been honoured as Patent Lawyer of the Year 2021 in Taiwan by 2021 *Corporate Intl Magazine Global Award*, Best Patent Prosecution Attorney (Taiwan) by *APAC Insider Legal Awards*, and Top 100 Women in Litigation 2020 by *Benchmark Litigation Asia-Pacific*.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000 ext. 2806
Email: hrchien@leeandli.com
URL: www.leeandli.com

Eddie Hsiung is licensed to practise law in Taiwan and New York. His practice focuses on M&A, securities, financial services, general corporate and commercial, start-ups, etc. He has participated in many corporate transactions (M&A, IPO, JV, cross-border investments) spanning a broad range of industries and areas, including TMT, bio-tech, big data, digital financial services, etc. In addition to the abovementioned traditional practice areas, he is familiar with legal issues regarding digital economy, digital transformation and the application of new technologies such as fintech, blockchain, virtual assets, AI, data protection, and is often invited to participate in public hearings, seminars, and panel discussions to provide advice to the government, regulators, legislators, university/research institutions in these areas on regulatory policies.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000 ext. 2162
Email: eddiehsiung@leeandli.com
URL: www.leeandli.com

Shih-I Wu has a dual background in biological engineering and law and specialises in handling intellectual property and civil disputes. Shih-I has a wealth of experience in litigation and administrative remedy procedures for patent applications, patent infringement and patent cancellation, as well as in civil and criminal litigation regarding trade secrets, copyrights, and trademark rights. She has undertaken significant trade secret cases and a landmark case concerning protection of computer software. She is also familiar with reviewing intellectual property contracts and consulting on related disputes, and has experience in intellectual property transaction negotiations, royalty audits, and tax exemption applications, as well as civil disputes, product liability and consumer protection, fair trade disputes, environmental law disputes, and labour disputes. Shih-I's writings on the practice of intellectual property rights have been published in both domestic and foreign journals.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000 ext. 2515
Email: shihiwu@leeandli.com
URL: www.leeandli.com

Lee and Li, founded more than half a century ago, is the largest law firm in Taiwan providing legal services in the Greater China area by collaborating with law firms and intellectual property agencies in Mainland China. Besides our headquarters in Taipei, we have offices in Hsinchu, Taichung and Kaohsiung, as well as strategic alliances in Beijing and Shanghai. Our services are performed by a total of around 860 employees, including nearly 200 Taiwan-qualified lawyers, 50 foreign lawyers, over 100 Taiwan patent agents/patent attorneys, more than 100 technology experts, and specialists in other fields such as Taiwan- and U.S.-certified public accountants, as well as the PRC patent attorneys and PRC-qualified lawyers of our strategic alliances.

www.leeandli.com

理律法律事務所
LEE AND LI
ATTORNEYS-AT-LAW
關懷・服務・卓越
we care・we serve・we excel

United Kingdom


Sally Shorthose


Toby Bond


Emma Drake


Pieter Erasmus

Bird & Bird LLP

1 Digital Health

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 digital health technologies in your jurisdiction?

The key emerging digital health technologies in the United Kingdom are as follows:

- **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 digital health for your jurisdiction?

The two core legal issues are:

- compliance, in the digital collation and handling of patient data, with the requirements of the UK's General Data Protection Regulation (**UK GDPR**) and the UK Data Protection Act 2018 (**DPA**); and
- compliance, in delivering digital health services, with the relevant UK healthcare regulatory regime. For example, in the case of telemedicine services, the regulatory regime is not yet fully updated to deal with the issues arising from the delivery of telemedicine services.

1.4 What is the digital health market size for your jurisdiction?

Certain sources estimate that the UK healthcare IT and digital market is currently valued at around £5 billion, although this is likely to grow significantly.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

Based on certain sources, examples of the more prominent digital health companies in the UK include:

- Babylon Health;
- Cera;
- Huma;
- Push Doctor;
- DoctorLink; and
- Lumeon.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

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 and the UK Medical Device Regulations 2002 (**MDR 2002**), as amended.

General legislation such as the Electronic Commerce Regulations 2002, the Consumer Rights Act 2015, and the Consumer Protection from Unfair Trading Regulations 2008 may also be relevant to digital health.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The use of personal data in digital health is regulated primarily by the UK 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 healthcare devices or software in particular?

Consumer health devices are, to the extent they are "medical devices", covered by the MDR 2002, as amended. All medical devices need to meet the applicable UKCA (UK Conformity Assessed) marking requirements in these regulations and must be registered. From 1 January 2023, CE marking can no longer be used in the UK and a UKCA mark shall be required in order to place a medical device on the Great Britain market. There will be separate requirements for certain medical devices placed on the Northern Ireland market, which is currently aligned with the EU regime.

All consumer devices are regulated by the UK General Product Safety Regulations 2005 and those other UKCA marking regulations which apply to the specific product, e.g. UK Electrical Equipment (Safety) Regulations 2016, etc. Evidence of compliance with applicable UKCA marking laws and regulations must be compiled and maintained by a nominated responsible person in the UK where the manufacturer is based outside the UK.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? 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 – Care Inspectorate Wales.
- Northern Ireland – The Regulation and Quality Improvement Authority.

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 UKCA marking regulations.

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

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, as amended. In September 2021 the MHRA announced its *Software and AI as a Medical Device Change Program* which will look to transform UK regulation in this area. What this means for the regulatory landscape in the UK is not yet clear but should become so in the coming years.

2.7 What regulations apply to Artificial Intelligence/Machine Learning powered digital health devices or software solutions and their approval for clinical use?

See directly above.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - Determining whether any of the devices used qualify as medical devices.
  - Determining whether such activity requires registration as a regulated activity.
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records; 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.
- **Wearables**
  - Determining whether any of the devices used qualify as medical devices.
  - Data protection compliance – assessing whether health data is collected by publishers or whether this is strictly limited to the local device, ensuring a lawful basis for processing (likely to be consent), ensuring privacy by design, explaining data processing to individuals, 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.
  - Data protection compliance. Similar issues to Telehealth.
- **Clinical Decision Support Software**
  Similar issues as for Telehealth.
- **AI/ML powered digital health solutions**
  Similar issues as for Telehealth.
- **IoT and Connected Devices**
  Similar issues as for Telehealth.
- **3D Printing/Bioprinting**
  - Liability allocation for poor outcomes – designer, manufacturer and/or HCP.
  - Contractual issues between the various suppliers and customers of services/products.
  - IP ownership issues.

- **Digital Therapeutics**
  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 lawful transmission, storing processing and use of data – and ensuring adequate consent to such use has been obtained. International data transfers remain a compliance hot topic.

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?

- Determining whether relevant data is personal data or has been sufficiently anonymised. Anonymisation is recognised as difficult to achieve in practice, and may reduce the utility of the relevant dataset. Simply removing identifiers may result in pseudonymous data, which is still caught by the UK GDPR.
- Confirming the roles of the parties involve in the processing – which parties are controllers or processors, and putting appropriate contracts in place.
- Identifying whether data is *concerning health* (and therefore subject to more stringent rules, as are other categories of "special category" data such as personal data on sex life or religion), *versus* less sensitive data that might for instance be collected for wellness purposes (e.g. step counts, sporting performance, etc.).
- Identifying the appropriate legal basis for processing data and obtaining any necessary consent.
- Carrying out a Data Protection Impact Assessment (**DPIA**), if required (as is likely) and ensuring that appropriate risk mitigations are put in place, including measures to ensure data minimisation, privacy by design, data retention limits and appropriate information security measures.
- Ensuring that any overlapping requirements related to rules on patient confidentiality are met.

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 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 UK GDPR, the DPA, and laws on confidentiality that vary between the different parts of the UK.

In addition, a substantial body of "soft law" tends to be imposed by other stakeholders' policies and contracts.

Additional legislation can apply for specific data uses, e.g. the Privacy and Electronic Communication Regulations (**PECR**) restricts non-consensual access to and storage of data on Internet-connected devices. Medical device or clinical trial laws further limit the use of personal data.

- The UK GDPR imposes significant restrictions on the use of health data without providing notice of that use and demonstrating an appropriate legal basis for processing the special category data. Often, explicit consents from individuals will be necessary. This must be specific, informed and freely given.
- Operators in England and Wales (in particular) must also deal with more restrictive requirements of "common law", particularly surrounding patient confidentiality and misuse of private information (**MoPI**). Without consent (which for confidentiality/MoPI purposes could be implied or explicit), or a clear statutory permission, only uses of patient personal data that are necessary for patient care or in the public interest, are permitted under English and Welsh law on confidentiality and MoPI.
- The UK GDPR also imposes 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 DPIAs, and generally, ensure that usage of personal data is fair, lawful and does not involve excessive amounts of data.
- The UK 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.
- Data protection law also includes laws that regulate the use of automated means to take significant decisions that have 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.
- Operators should be aware that the UK Government has recently consulted on changes to UK data protection law, which may lead to changes to the UK GDPR and the DPA.

4.4 Do the regulations define the scope of data use?

The 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 4.3 above, there are overlapping restrictions under contract, soft law and confidentiality/MoPI rules which may affect the need to obtain consent.

Although this consent does not have to meet the same standard as explicit consent under the UK GDPR, care should be taken (and specialist advice obtained) to ensure that, where relying on UK GDPR/DPA grounds for processing personal data, 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 UK 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 UK 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 travelling internationally, then the UK 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), and onward transferees.

By contrast, UK data protection laws generally have little impact on contracts with individuals; data protection-related matters should be dealt with outside of those contracts (e.g. through dedicated privacy notices, and stand-alone consent requests).

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The legality of planned and future uses of personal data will be conditional on ensuring that notices, consents, contracts and/or lawful exemptions cover all anticipated uses – or expose an organisation to significant investigations and civil and/or criminal liability. In parallel, failure to secure appropriate IP rights from rights holders can expose the organisation to a risk of being sued by that organisation, and/or additional criminal liability under the DPA (if the data is personal data).

5 Data Sharing

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

The sharing of personal data means that confidentiality and privacy concerns will often be more acute than simply using data within a single organisation. For example, in England and Wales, even greater attention needs to be paid to the existence of a care need, consent, statutory permission and/or a public interest justification for the proposed data sharing if it involves patient data processed for the purposes of providing care. 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.

Key aspects of the data sharing may need to be explained to individuals, in accordance with the GDPR's transparency obligations.

Finally, sharing personal data across borders – even just by providing remote access to it – raises GDPR data transfer compliance issues.

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?

The 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.

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 are payable on application and renewal. Protection lasts 20 years from the 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 (**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 rules or laws that apply to academic technology transfers in your jurisdiction?

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).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

Following the decision in *Stephen L Thaler v The Comptroller-General of Patents, Designs And Trade Marks* [2021] EWCA 1374, an AI device cannot be named as an inventor of a patent in the UK. In October 2021, the UKIPO issued a public consultation on whether the Patents Act should be amended to permit an AI system to be named as an inventor or whether the definition of inventor should be expanded to include humans responsible for an AI system which devises inventions. The outcome of the consultation is expected during the course of 2022.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

Government funding for innovation is available in the UK. This funding is classed as a subsidy and therefore must be consistent with WTO rules, the EU-UK Trade and Cooperation agreement and other bilateral UK Free Trade Agreements.

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 themself in an invidious situation if complete clarity is set out regarding the permitted uses a joint owner may have over the IP.

There may be 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 healthcare and non-healthcare companies?

As with any agreement, the allocation of rights and obligations should be set out clearly, 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.

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. Data provisions in AI service agreements should also consider the status of meta-data which may be generated through customer interactions with the system.

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, although the protection applies to the particular expression of ideas and principles which underly an algorithm and not to the ideas and principles themselves. 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.

In October 2021, the UKIPO issued a public consultation seeking views on possible reforms to the protection of computer generated works in the UK. The options under consideration included retaining the existing position under Section 9(3) CDPA, removing protection for computer generated works, or replacing Section 9(3) with a new and narrower form of protection with a limited duration, e.g. five years from creation. The outcome of the consultation is expected during 2022. While algorithms are not directly mentioned in the consultation, changes to the protection of computer generated works could potentially affect the analysis set out above.

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.

Issues regarding use of training data commonly arise in the context of AI service agreements. An AI service provider will commonly wish to re-use data received from a customer during the course of providing the service to further improve the AI system which is used to provide the service, or potentially to develop new AI models for use in a different context. Customers may resist contractual terms which permit this re-use of their data for these purposes, considering it to be a net value transfer from them to the service provider. Provisions relating to the use of derived data and meta-data, anonymisation and data retention post-termination may all be affected by this issue.

9 Liability

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

Liability for adverse outcomes in digital health is governed both by the law of contract (where services are delivered in accordance with a contract) and by the common law of tort/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 (**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?

Previously, under EU law (the Rome Regulations), generally, UK national (English and Welsh, Scottish or Northern Irish) laws have applied 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. In accordance with retained EU law, the situation is not expected to change significantly post-Brexit, at least in the short term.

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-healthcare companies should consider before entering today's digital healthcare 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 healthcare ventures?

When considering a target:

- Ensure that procedures are in place for compliance with relevant areas, especially data protection, patient confidentiality, MDR and WEEE.
- 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?

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

- Generally, the use of digital health solutions in the UK is well established. The COVID-19 pandemic has increased the prevalence of digital health solutions.
- However, regarding the delivery of telemedicine services specifically, there remains some legal uncertainty because the UK healthcare regulatory environment is not yet fully updated to deal with the issues arising from the delivery of telemedicine services.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

While not a clinician certification body *per se*, in the UK, the *Association of British HealthTech Industries* (**ABHI**) plays a key role representing the industry to stakeholders, such as the Government, NHS and regulators.

Lobbying in the UK is less formalised, but ensuring that the particular digital health solutions meet certain criteria such as the NICE Evidence standards framework for digital health technologies would improve the likelihood of widespread adoption.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

This would depend on the product in question. From an England perspective, while there may not yet be specific publicly funded provision of general health apps *per se* direct to patients, the provision of, e.g. telemedicine may, under certain circumstances, be funded via the NHS. This would be an area to keep a close watch on since the recent launch of the NICE *Office for Digital Health*, which intends to, amongst other things, work with strategic partners to improve digital health approval pathways and reimbursement policy.

Acknowledgment

The authors would like to thank Callum Granger for his invaluable assistance in the writing of this chapter. Callum is a trainee solicitor at Bird & Bird LLP, based in 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

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

Emma Drake is a senior associate in Bird & Bird's Privacy and Data Protection Group. She works with a variety of healthcare and life science clients, from traditional pharmaceutical companies to health informatics providers to new entrants handling personal data in the context of wellness apps or new technology. She has helped clients on diverse topics spanning application of research exemptions, anonymisation, assessing the compliance of new medical technologies, patient support programmes and the processing of data for pharmaceutical regulations such as pharmacovigilance or restrictions under the ABPI code.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7415 6728
Email: emma.drake@twobirds.com
URL: www.twobirds.com

Pieter Erasmus is an associate in the Intellectual Property Group in London, with a focus on regulatory and commercial matters primarily in the life sciences and healthcare sectors. Having a keen interest in all things life sciences and healthcare, he specialises primarily in providing regulatory advice in relation to a broad range of matters in these fields, including pharmaceuticals, medical devices, general healthcare, clinical trials, marketing and advertising of health products, etc. Pieter's experience further includes corporate and commercial work, including transactional work and the drafting of a wide range of general and bespoke commercial agreements in the life sciences and healthcare sectors. Before joining Bird & Bird in 2019, he spent over six years working at the Johannesburg offices of Africa's largest law firm.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7905 6217
Email: pieter.erasmus@twobirds.com
URL: www.twobirds.com

USA

Norton Rose Fulbright


Roger Kuan


Jason Novak

1 Digital Health

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

Digital health is a technology sector that is a convergence of high technology with healthcare. The result is a highly personalised healthcare system that is focused on data-driven healthcare solutions, individualised delivery of therapeutics and treatments to patients powered by information technologies that enable seamless integration and communication between patients, providers, payors, researchers and health information depositories.

1.2 What are the key emerging digital health technologies in your jurisdiction?

The key technology areas in digital health are:
- Personalised/Precision Medicine (treatments tailored to an individual's uniqueness).
- Clinical Decision Support Tools (analytics tools used to assist physician decision-making).
- Remote Patient Monitoring and Delivery of Care (e.g., Internet of Medical Things (IoMT), Telemedicine, Virtual Healthcare, mobile applications, wearables, etc.).
- Big Data Analytics (clinically relevant inferences from large volumes of medical data).
- Artificial intelligence/machine learning (AI/ML)-powered Healthcare Solutions (e.g., diagnostics, digital therapeutics, intelligent drug design, clinical trials, etc.).
- Robot Assisted Surgery (precision, reduced risk of infection).
- Digital Hospital (digital medical information management, optimised hospital workflows).
- Digital Therapeutics (use of digitally enabled devices or software to provide therapeutic treatment to patients).

1.3 What are the core legal issues in digital health for your jurisdiction?

Some core legal issues to digital health are:
- Patentability of digital health technologies especially with respect to innovations in software and diagnostics.
- Data privacy and compliance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Consumer Privacy Act (CCPA), and the federal Health Information Technology for Economic and Clinical Health Act (HITECH Act).
- The Federal Food, Drug and Cosmetic Act (FFDCA, FDCA, or FD&C Act), which regulates food, drugs, and medical devices. The FFDCA is enforced by the U.S. Food and Drug Administration (FDA) which is a federal agency under the U.S. Department of Health and Human Services (DHHS). Relevant FDA regulations and programmes related to digital health include 510(k) certification, Premarket Approval (PMA), Software as a Medical Device (SaMD), Digital Health Software Pre-certification Program (Pre-Cert Program), and Laboratory Developed Test (LDT) regulated under the Clinical Laboratory Improvement Amendments (CLIA) programme.
- Practice of Medicine Laws that relate to licensure of physicians who work for telemedicine and virtual health companies. These can be state-specific or part of the Interstate Medical Licensure Compact Commission (IMLCC), which regulates the licensure of physicians to practice telemedicine in the list of Member States.
- Stark Law and Anti-Kickback Statutes that apply to telemedicine and virtual health providers who enter into business arrangements with third parties that incentivise care coordination and patient engagement.

1.4 What is the digital health market size for your jurisdiction?

Depending on the source and how they define the digital health market estimates of the digital health market size in the USA for 2020 range from a low of $39.4 billion to a high of $181.8 billion.

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

The five largest digital health companies in the USA are as follows:
- Optum.
- Cerner Corporation.
- Cognizant Technology Solutions.
- Change Healthcare.
- Epic.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

In the U.S., the Federal Food, Drug and Cosmetic Act and subsequent amending statutes (FFDCA, FDCA or FD&C Act)

is the principal legislation by which digital health products that meet the definition of medical devices are regulated.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinic Health Act (HITECH ACT) is a core healthcare regulation related to digital health. HIPAA sets forth the federal privacy and security requirements for how certain entities must safeguard protected health information (PHI) (inclusive of electronic PHI or ePHI) and how to handle security breaches of PHI or ePHI. In the U.S., individual states may also have state-specific healthcare privacy laws that pertain to their state residents that might apply to digital health offerings in a particular state and that may also be stricter than HIPAA.

In addition, a provider of digital healthcare will also be subject to various healthcare laws and regulations designed to promote transparency and prevent fraud, abuse and waste. Such laws and regulations to the extent applicable may include, but are not limited to: the federal Anti-Kickback Statute; the Ethics in Patient Referrals Act (or "Stark Law"); the federal False Claims Act, laws pertaining to improper patient inducements; federal Civil Monetary Penalties Law; and state-law equivalents of each of the foregoing.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Consumer devices are regulated under the statutory and regulatory framework of the FDCA as applies to all products that are labelled, promoted or used in a manner that meets the definition of a "device" under the FDCA. Additionally, the regulations that apply to a given device differ depending on the regulatory class to which the device is assigned and is based on the level of control necessary to ensure safety and effectiveness: Class I (general controls); Class II (general contracts and special controls); and Class III (general controls and premarket approval (PMA)). The level of risk that the device poses to the patient/user is a substantial factor in determining its class assignment.

From a consumer standpoint, digital health devices and offerings are also subject to laws and regulations that protect consumers from unfair and deceptive trade practices as enforced on a federal level by the Federal Trade Commission.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

In the United States, the U.S. Department of Health and Human Services (HHS) regulates the general health and safety of Americans through various programmes and divisions, including the U.S. FDA, Centers for Medicare and Medicaid Services (CMS), Office of Inspector General (OIG) and Office for Civil Rights (OCR), among many others.

The FDA is the principle regulatory body charged with administering and enforcing the provisions of the Federal Food, Drug & Cosmetic Act, including those that relate to medical devices and Software as a Medical Device (SaMD). The FDA's jurisdiction covers all products classified as food, dietary supplements, drugs, devices or cosmetics, which have been introduced into interstate commerce in the United States.

In respect of the FDA's regulatory review of digital health technology, the Digital Health Center of Excellence (a part of the U.S. Food and Drug Administration based in the Center for Devices and Radiological Health) aligns and coordinates digital health work across the FDA providing the FDA with regulatory advice and support to assist the FDA in its regulatory review of digital health technology.

The Digital Health Center of Excellence provides services in the following functional areas of digital health:

- Digital Health Policy and Technology Support and Training.
- Medical Device Cybersecurity.
- AI/ML.
- Regulatory Science Advancement.
- Regulatory Review Support and Coordination.
- Advanced Manufacturing.
- Real World Evidence and Advanced Clinical Studies.
- Regulatory Innovation.
- Strategic Partnerships.

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

The FDA has expressed its intention to apply its regulatory oversight to only those digital health software functions that are medical devices and whose functionality could pose a risk to a patient's safety if the device were to not function as intended. From a digital health perspective, this is a key area of enforcement particularly in regard to digital health medical devices that are being marketed without the necessary FDA clearances or approvals in violation of applicable FDCA regulations.

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

SaMD is regulated by the FDA and is defined by the International Medical Device Regulators Forum (IMDRF) as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device". SaMD can be used across a number of technology platforms including, medical device platforms, commercial platforms and virtual networks. For example, SaMD includes software with a medical purpose that operates on a general-purpose computing platform.

If the software is part of a hardware medical device, however, it does not meet the definition of software as a medical device and is not regulated by the FDA. Examples include: software that relies on data from a medical device, but does not have a medical purpose (e.g., encryption software); or software that enables clinical communication such as patient registration or scheduling.

Consistent with the FDA's existing oversight approach that considers functionality of the software rather than platform, the FDA has expressed its intention to apply its regulatory oversight to only those software functions that are medical devices and whose functionality could pose a risk to a patient's safety if the device were to not function as intended. For software functions that meet the regulatory definition of a "device" but pose minimal risk to patients and consumers, the FDA exercises its enforcement discretion and will not expect manufacturers to submit premarket review applications or to register and list their software with the FDA. Examples of such minimal risk software includes functionality that helps patients self-manage their

medical condition without providing specific treatment suggestions or that automate simple tasks for healthcare providers. The FDA publishes a more detailed list of examples of device software functions that are not the focus of FDA oversight.

In regard to the clinical evaluation of SaMD, the FDA issued the *Software as a Medical Device: Clinical Evaluation* final guidance to describe an internally agreed upon understanding of clinical evaluation and principles for demonstrating the safety, effectiveness, and performance of SaMD among regulators in the International Medical Device Regulators Forum. The guidance sets forth certain activities SaMD manufacturers can take to clinically evaluate their SaMD.

It should be noted that the FDA considers mobile medical apps (mHealth apps) to be medical devices if they meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated device. The FDA has published guidance that explains the FDA's oversight of mobile medical apps entitled the *Policy for Device Software Functions and Mobile Medical Applications Guidance*.

2.7 What regulations apply to Artificial Intelligence/Machine Learning powered digital health devices or software solutions and their approval for clinical use?

Digital health devices and software solutions that are powered by AI and ML technologies are subject to FDA regulations and related review. In April of 2019, the FDA published the "*Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI//ML)-Based Software as a Medical Device (SaMD) – Discussion Paper and Request for Feedback*". The FDA remarked in its proposal that "[t]he traditional paradigm of medical device regulation was not designed for adaptive AI/ML technologies, which have the potential to adapt and optimize device performance in real-time to continuously improve healthcare for patients". The FDA also described in the proposal its foundation for a potential approach to premarket review for AI and ML-driven software modifications.

In January 2021, the FDA published the "*Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan*" that included the FDA's plan to update its proposed regulatory framework through a five-part action plan that addresses specific stakeholder feedback. The five-part plan includes the following actions:

i. Develop an update to the proposed regulatory framework presented in the AI/ML-based SaMD discussion paper, including through the issuance of a Draft Guidance on the Predetermined Change Control Plan.
ii. Strengthen FDA's encouragement of the harmonised development of Good Machine Learning Practice (GMLP) through additional FDA participation in collaborative communities and consensus standards development efforts.
iii. Support a patient-centreed approach by continuing to host discussions on the role of transparency to users of AI/ML-based devices. Building upon the October 2020 Patient Engagement Advisory Committee (PEAC) Meeting focused on patient trust in AI/ML technologies, hold a public workshop on medical device labelling to support transparency to users of AI/ML-based devices.
iv. Support regulatory science efforts on the development of methodology for the evaluation and improvement of machine learning algorithms, including for the identification and elimination of bias, and on the robustness and resilience of these algorithms to withstand changing clinical inputs and conditions.
v. Advance real-world performance pilots in coordination with stakeholders and other FDA programmes, to provide additional clarity on what a real-world evidence generation programme could look like for AI/ML-based SaMD.

The FDA highlighted that its work in this area will be coordinated through the Center for Devices and Radiological Health's new Digital Health Center of Excellence.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - State-specific practice of medicine licensing laws and requirements.
  - Data privacy laws including HIPAA, CCPA and HITECH Act with respect to health data that is collected from patients during consultation.
  - Data rights to health data collected from patients during consultation.
  - FDA regulatory issues such as SaMD, 510k certification and PMA.
  - Stark Law and Anti-Kickback Statutes.
- **Robotics**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with respect to health data that is collected and used to train software used to operate the robotic device.
  - Tort liability (products liability or negligence theories) for injuries sustained by patients during surgery.
  - FDA regulatory issues such as 510k certification and PMA.
- **Wearables**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards to health data that is collected by devices.
  - Data rights to health data that is collected from device wearers.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer seeks to make diagnostic or therapeutic claims for their devices.
- **Virtual Assistants (e.g. Alexa)**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards to voice and WiFi signal data that is collected by the virtual assistant.
  - Data rights to the voice and WiFi signal data that is collected by the virtual assistant.
  - FDA regulatory issues such as SaMD, 510k, and PMA if manufacturer seeks to make diagnostic or therapeutic claims for the virtual assistant.
- **Mobile Apps**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards to health data that is collected by the mobile app.
  - Data rights to the health data that is collected by the mobile app.
  - FDA regulatory issues such as SaMD, 510k and PMA if manufacturer seeks to make diagnostic or therapeutic claims for the mobile app.
  - Tort liability (products liability or negligence) for injuries sustained by patients using mobile apps for diagnostic or therapeutic purposes.
  - Issues related to the patentability of software or diagnostics inventions.

- **Software as a Medical Device**
  - FDA regulatory issues such as SaMD, 510k and PMA if manufacture makes diagnostic or therapeutics claims for the software. Unique issues with evaluating safety and efficacy of software used to diagnose or treat patients.
  - Issues related to patentability of software of diagnostics inventions.
- **Clinical Decision Support Software**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards to health data that is used in the software.
  - FDA regulatory issues such as SaMD, 510k and PMA if developer seeks to make diagnostic or therapeutic claims for the software.
  - Tort liability (products liability or negligence) for injuries sustained by patients using the software for diagnostic or therapeutic purposes.
  - Issues related to the patentability of software or diagnostics inventions.
- **AI/ML powered digital health solutions**
  - Inventorship issues with inventions arising out of AI/ML algorithms.
  - Clinical adoption of AI/ML software that is used in a clinical setting.
  - FDA regulatory issues such as SaMD, 510k, and PMA if manufacturer makes diagnostic or therapeutics claims for the AI/ML-powered software. Unique issues with evaluating safety and efficacy of AI/ML-powered software used to diagnose or treat patients.
  - Data rights issues related to the data sets that are used to train AI/ML software with. It is even more complicated if the training data set includes data sets from multiple parties with differing levels of data rights.
- **IoT and Connected Devices**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards to health data that is collected by the IoT connected devices.
  - Data rights to the health data that is collected by the IoT connected devices.
- **3D Printing/Bioprinting**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to handling of patient imaging data used as 3D printing templates.
  - FDA regulatory issues such as SaMD, 510k, PMA and Biologics License Application (BLA) depending on whether the manufacturer is making and selling rendering software, printing equipment and bioink with cells or other biological compositions.
- **Digital Therapeutics**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards to health data that is used in or collected by the software and/or devices.
  - FDA regulatory issues such as SaMD, 510k and PMA if developer seeks to make therapeutic claims for the software and/or devices.
  - Tort liability (products liability or negligence) for injuries sustained by patients using the software or devices for therapeutic purposes.
  - Issues related to the patentability of software or diagnostics inventions.
- **Natural Language Processing**
  - FDA regulatory issues if the natural language processing (NLP) software is used as part of a medical device or SaMD used as a diagnostic or therapeutic purpose.
  - Tort liability (products liability or negligence) for injuries sustained by patients using these apps or devices, that incorporates the NLP software, for diagnostic or therapeutic purposes.

3.2 What are the key issues for digital platform providers?

The key issues for digital platform providers are:

- Compliance with data privacy laws including HIPAA, CCPA and HITECH Act with regards to health data that is collected by the providers.
- Obtaining data rights to the health data collected from customers/patients by complying with informed consent requirements.
- Data sharing and IP provisions in agreements.
- Tort liability (products liability of negligence) for injuries sustained by patients using these platforms for diagnostic or therapeutic purposes.
- Issues related to the patentability of software or diagnostics inventions.

4 Data Use

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

Some of the key issues to consider for the use of personal data are:

- **What type of personal data is it?** If it is PHI, it would thereby be subject to HIPAA. Contrast this with wellness data, for example, which would appear to be health-related but in reality, is separate and distinct and, therefore, not regulated by HIPAA. Of course, personal data in general is subject to various, state, federal, and international data privacy laws.
- **What is the intended purpose of this data?** Defining this purpose early and often is essential as it will become core to the metes and bounds of the data transaction and will help with the initial undertaking of seeking appropriate (patient) consents, which is far easier to do at the outset.
- **What are potential secondary uses of the data?** Defining secondary uses up front is also important as a data user must maximise the value of the data transaction. Failing to set the expectation early may result in a data transaction of limited scope, forcing a data user to either seek amendment to the existing transaction or the need for a second agreement. In either case, leverage in negotiation will quickly pivot to the data holder, who will now have a clear idea of the importance to the data user of these secondary users.
- **Where is the data coming from and where is it going?** To answer this, detailed data maps need to be developed, tracing the path of data across various states and nations, thereby identifying the jurisdictions that will define the scope of data compliance requirements for a data user. As stated above, each impacted territory, whether state or country, may have unique data compliance (data privacy) laws that must be accounted for in executing the data strategy. Of note, data mapping is a requirement under several of the potentially applicable healthcare laws and as such, it is factored into several parts of the data strategy.

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

Assuming the data under consideration is PHI, in dealing with

HIPAA, a threshold determination is whether one is an entity subject to HIPAA (referred to as a "Covered Entity"), or a "Business Associate" of said Covered Entity by way of providing certain services for the Covered Entity. Covered Entities, aside from providers of healthcare that bill through claims, include, for example, government healthcare programmes (e.g., Medicare, Medicaid, military health programmes, veteran health programmes), health maintenance organisations (HMOs), employee sponsored health plans, and health insurance companies. Business Associates are parties (person or entity) that are not part of a Covered Entity workforce but, by virtue of acting on behalf of, or providing certain services to, a Covered Entity, receive access to PHI that is in the possession of the Covered Entity and which the Covered Entity has responsibility for.

4.3 Which key regulatory requirements apply?

HIPAA is the primary and fundamental U.S. federal law related to protecting patient health information. In relation to HIPAA, the HITECH, signed into law in 2009, further increased patient rights by financially incentivising the adoption of electronic health records and increased privacy and security protection, and also increasing penalties to covered entities and their business associates for HIPAA violations. The CCPA, enacted in 2018, is an example of a state statute primarily focused on addressing the enhancement of privacy rights and consumer protection for that state's residents. Similar applicable laws exist in many U.S. states. Especially for data transactions with the EU, the General Data Protection Regulation (GDPR), in force since May 2018, protects natural persons in relation to the processing and movement of personal data.

4.4 Do the regulations define the scope of data use?

Generally, yes, and particularly, the regulations concerning PHI, HIPAA and HITECH define the allowable scope of data use.

4.5 What are the key contractual considerations?

Key contractual considerations depend on what is being contracted. For example, for a data transaction involving entities as part of collaborative research, intellectual property rights arising out of the research, as well as primary and secondary uses of the data, are essential to clearly define. Field restriction language can also become important, as it can minimise the impact of a data transaction agreement to a company's overall business strategy. With PHI involved, if an involved entity has been identified as a business associate, then a Business Associate Agreement may be needed between the business associate and covered entity. With non-PHI involved, data processing agreements may still be needed for handling data, even though it is not subject to HIPAA. Other potentially important terms include terms addressing data breaches, data handling during and after the agreement period, and associated representation/warranty language associated with any breach.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Securing comprehensive rights is extremely important. Healthcare data is exceptionally valuable – valuable to both the patient and the company that is able to procure such data. Given its criticality, one must have permission to use healthcare data for a desired purpose. Regardless of whether the healthcare data is generated or acquired by the data user, the data user must have the consent of the data's ultimate owner, i.e., the patient, to use that healthcare data. In cases where healthcare data is acquired from a third party, the data user must also have the consent of the third party to use the healthcare data for a desired purpose. Often, consent from a third party (e.g., a healthcare data warehouse or aggregator) comes in the form of a data transaction, whereby said data user will usually remunerate the third party to acquire the healthcare data for the desired purpose. Of course, the consent between data owner and data user will come via the data owner providing consent to this third party to transact the data to parties such as the data user. It is worth noting that a healthcare data warehouse or aggregator does not solely mean data mines such as personal genomics companies 23andMe and Ancestry. It also includes traditional entities such as hospitals and hospital systems, universities, research institutes and pharmaceutical companies. Consent can come in a variety of ways, but it is critical to be able to demonstrate such consent for any downstream data use.

5 Data Sharing

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

Key issues include data privacy and security generally, regardless of whether the information is personal health information or not. For personal data in general, as discussed herein, entities dealing in data must consider the regulatory requirements across different jurisdictions. For U.S. data sharing, federal and state laws must be considered. For international data sharing, ex-U.S. regulatory schemes must fold into a data sharing strategy.

When the personal data is PHI, the regulatory requirements only increase, with federal laws such as HIPAA and HITECH to consider.

From a personal standpoint, each individual must recognise their own personal right to their own data, and must consider agreeing to consent agreements that may provide entities with the right to transact one's personal data beyond the scope said individual might desire.

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

As discussed herein and previously, when data is PHI and subject to federal regulations such as HIPAA and HITECH, entities that qualify as Covered Entities and Business Associates may have to execute Business Associate Agreements to be in proper standing, and may have to ensure that all associated parties involved meet the obligations imposed by federal laws for the handling of PHI.

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

Please see section 4.

6 Intellectual Property

6.1 What is the scope of patent protection?

As relevant to digital health, current U.S. patent law is generally unfavourable towards the subject matter patentability of software and diagnostics inventions. As such, successfully navigating the subject matter patentability hurdle is the first step to protecting digital health solutions. Recent U.S. Supreme Court and Federal Circuit cases have begun to chip away at this hurdle for diagnostics innovation (See *Hikma Pharmaceuticals USA Inc. v. Vanda Pharmaceuticals Inc.* (https://www.scotusblog.com/case-files/cases/hikma-pharmaceuticals-usa-inc-v-vanda-pharmaceuticals-inc/) and *CardioNet, LLC v. InfoBionic, Inc.* (https://law.justia.com/cases/federal/appellate-courts/cafc/19-1149/19-1149-2020-04-17.html)) and the current expectation is that future cases will continue to swing towards affirming protection for this important class of innovation. In addition to satisfying the subject matter hurdle, novelty and non-obviousness are also required for patentability.

The term of utility patent protection (with certain exceptions) is 20 years (15 years for design patents) from the date of filing the application. A patent gives the patent owner an affirmative right to exclude others from making, using or selling the patented invention.

6.2 What is the scope of copyright protection?

For digital health solutions, copyright protects the software source code and object code as works 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 U.S. has a formal process to register copyrights, which is a prerequisite for commencing a copyright infringement action. Registered copyrights are eligible for "statutory damages" under the Copyright Act which can help mitigate the difficulties in establishing the monetary value damages due to the copyright infringement. Copyrights that are registered within five years of publication establishes *prima facie* evidence of the validity of the copyright and facts stated in the copyright registration certificate. Also, the burden of proof of non-infringement shifts to the alleged infringer.

To register software source code (or object code) or a database with the U.S. Copyright Office (a part of the Library of Congress) a "registration deposit" copy of the software code or database must be deposited that meets the requirements under the Act. 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 can be used to protect formulas, practices, processes, designs, instruments, patterns, or compilations of information that is not generally known to the public and have inherent economic value. Trade secrets have no fixed term but require the owner to appropriately mark the information and to put in appropriate safeguard measures to guard the information from being released to the public. However, unlike patents, trade secrets cannot prevent independent development of the trade secret information.

6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

Most academic institutions require their professors, researchers and students to assign any IP they develop with the institution's resources or funding to back them. In some instances, the institutions, applicable departments and the professor/researcher enter into separate royalty-sharing agreements.

The IP is typically out-licensed to third parties for commercialisation on terms that may include: royalties; upfront payments; milestone payments; and equity in the licensee company.

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

SaMD, which the FDA defines as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device" can be protected by patents, copyrights and/or trade secrets. SaMD source code and objects can be copyrightable and trade secret subject matter (provided that they are appropriately marked and appropriate protections are put into place to ensure that they're not released to the public). An SaMD can also be protectable by patents if it meets U.S. subject matter patentability requirements and is novel and non-obvious over the prior art.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

In the United States, both the courts (in *Stephen Thaler v. Andrew Hirshfeld*, E.D.Va., 2021) and the U.S. Patent and Trademark Office (USPTO) have ruled that an AI machine cannot be an "inventor" for purposes of the United States Patent Act (35 U.S. Code).

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

In the U.S., the Bayh-Dole Act of 1980 (35 U.S.C. § 200–212) deals with inventions arising from federal government-funded research. Before the enactment of the Bayh-Dole Act, the government's consistent position was that the results of any research and development funded with taxpayer's money should be in the public domain and freely available to the public.

The Bayh-Dole Act permits qualified small businesses and non-profits to retain title to "subject inventions" arising out of federal funded research providing that they comply with the following conditions: (1) the federal government receives a licence in subject inventions; (2) the private party has properly notified the government of the subject inventions; (3) the preference for U.S. industry that is found in all technology transfer programs is included; and (4) the federal government retains "march-in rights". Within this framework, a "subject invention" is any invention of a qualified private party (i.e., small business or non-profit) conceived or first actually reduced to practice in the performance of work under a funding agreement. Whereas, "march-in rights" permits the federal government to order a private party to grant a compulsory licence to a third party (including competitors) when they make a determination that the private party has not: (1) taken effective steps to achieve practical application of the invention within a reasonable time; (2) reasonably satisfied national health and safety needs; (3)

reasonably satisfied regulatory requirements for public use; or (4) received the required permission from the government under the U.S. industry preference provision before licensing.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Collaborations are commonplace in digital health and can generally be grouped into two categories: data driven; and technology driven.

In data-driven digital health collaborations, the parties are interested in granting, acquiring or sharing access to data that is used to power digital health solution(s).

Typical data driven collaboration scenarios are:

- A healthcare institution (e.g., hospital system, hospitals, clinics, community health organisations, etc.) sharing their patient data (typically patient medical records, biological samples used to generate data, questionnaires, etc.) with a company that utilises the data to discover or power their digital health solution(s).
- A university or non-profit research organisation sharing their research data with a company that utilises the data (typically genomic, proteomic, microbiome, study results, etc.) with a company that utilises the data to discover or power their digital health solution(s).
- Companies sharing patient or research data where the data flows from one company to the other or between the companies to discover or power their digital health solution(s).

In technology-driven digital health collaborations, the parties are interested in either obtaining technology from one another or sharing their collective technologies to develop the digital health solution(s).

Typical technology-driven collaboration scenarios are:

- A university or non-profit research organisation sharing their technology or know-how with a company that utilises that technology their digital health solution(s).
- Companies sharing technology or know-how to develop combined digital health solution(s).

Ownership of intellectual property rights (e.g., patents, copyrights, technical know-how, research results/data, etc.) to the collaborative improvements that result from the shared data and technologies can be governed by U.S. intellectual property laws and/or in the terms of the agreement between the parties. Although the default stance is typically joint ownership, data owners have unique negotiation leverage to insist that they own the intellectual property rights (with the data recipient being granted a licence or option to those rights) since their data is the core asset in the collaboration.

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

The most important legal considerations to pay attention to in agreements between healthcare and non-healthcare companies are data privacy compliance and data rights.

With respect to data privacy compliance, the parties need to pay attention to their respective roles and responsibilities in the agreement as it relates to compliance with HIPAA and patient-informed consent requirements. Failure to properly develop and/or execute processes that are compliant with HIPAA or informed consent requirements can result in patient data that is tainted, which will encumber its use by the parties.

Data rights is another important consideration in this type of agreement where data (e.g., patient medical records, questionnaires, etc.) is typically owned by the healthcare company which then shares it with the non-healthcare company. It is important for the non-healthcare company to secure the data rights it needs from the healthcare company so that they can use the data for what they need it for and to have the healthcare company warrant or represent that they have properly secured the rights to the data from their patients.

8 AI and Machine Learning

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

AI, particularly ML, is used in a variety of ways to enable a myriad of digital health solutions. It has transformed the way healthcare data is processed and analysed to arrive at predictive insights that are used in applications as diverse as new drug discovery, drug repurposing, drug dosing and toxicology, clinical decision support, clinical cohort selection, diagnostics, therapeutics, lifestyle modifications, etc.

Precision medicine models that are powered by big data analytics and AI/ML can ensure that an individual's uniqueness (e.g., genome, microbiome, exposome, lifestyle, etc.) factors into the prevention and treatment (e.g., therapeutics, surgical procedures, etc.) of disease condition(s) that the individual is suffering from. An example of this would be companion diagnostic tests that are used to predict an individual's response to therapeutics based on whether they exhibit one or more biomarkers.

AI/ML algorithms trained to predict biological target response and toxicity can also be used to design novel (i.e., non-naturally occurring) chemical structures that have strong binding characteristics to a biological target with correspondingly low chemical and/or systemic toxicity. This promises to shorten the initial drug target discovery process as it moves away from looking for the proverbial "needle in a haystack" to a "lock and key" approach and will likely lead to drugs that have greater efficacy and less side effects for larger groups of patients.

8.2 How is training data licensed?

The rights to training datasets are typically specified in the agreements between the parties sharing the data. Data rights can be licensed in the same manner as other types of intellectual property rights. That is, it can be treated as a property right (either under copyrights, trade secrets, or as proprietary information) that can be limited by use, field, jurisdiction, consideration (monetary or in kind), etc. As a result, training data licence agreements can be structured with terms that can apportion ownership and rights (e.g., intellectual property, use, etc.) to the trained ML algorithm and any insights that it generates.

Some representative examples are:

- A healthcare system gives a ML drug discovery company access to its data set (i.e., patient medical records) and requires a non-exclusive licence to use the ML algorithm that was trained with its dataset for any purpose and joint ownership of any intellectual property rights on clinical insights generated by the ML algorithm.
- A pharmaceutical company gives its data set (i.e., clinical trial data) to a ML data analytics company as part of a collaboration and limits the use of the data for the field of hypertension and asks for an option to exclusively license any intellectual property rights arising from insights

generated by the ML algorithm trained with its data set.
- Two pharmaceutical companies agree to combine their data sets (i.e., Car-T research data) with one another and carve out specific fields (e.g., leukaemia, lymphoma, breast cancer, etc.) that each of them can use the combined data set for.

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

Current U.S. law requires that patents and copyrights can only be owned by human inventors and authors, respectively.

For patents, 35 U.S.C. §100, the Manual of Patent Examining Procedure (MPEP) and recent Federal Circuit cases (*Beech Aircraft Corp. v. EDO Corp.*, 990 F.3d 1237, 1248 (Fed. Cir. 1993); *Univ. of Utah v. Max-Planck-Gesellschaft zur Forderung der Wissenschaften e.V.*, 743 F.3d 1315 (Fed. Cir. 2013)) have held that only natural persons can be inventors for patents.

For copyrights, §306 of the Compendium of U.S. Copyright Office Practice states that "[t]he U.S. Copyright Office will register an original work of authorship, provided that the work was created by a human being".

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

A variety of different commercial considerations must be addressed when licensing data for use in ML for digital health solutions.

They are:
- Data Set Definition.
- The contents of the data (e.g., genomic, proteomic, electronic health records, etc.) being shared.
- The type of data (e.g., PHI, deidentified, anonymised, etc.) that is being shared.
- The file format of the data being shared.
- Data Use Case.
- Data used to train ML algorithm of digital health solution.
- Geographic location(s) for data use.
- Fields (e.g., oncology, ophthalmology, etc.) that the data can be used in.
- Data Rights.
- Ownership of the data and subsequent data generated from the data.
- Amount of time that the data can be used for.
- Sub-licensing rights.

9 Liability

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

Theories of liability include: contract breach (e.g., data agreements, data transaction, consent agreements); violation of U.S. federal, U.S. state, and ex-U.S. laws related to the protection of patient health information and personal data generally; negligence (e.g., by the product provider, the health provider, or the payer); product liability and Consumer Protection Law in the U.S. and abroad; Corporate Practice of Medicine; and Anti-Kickback laws (even with recent legislation increasing safe harbour).

9.2 What cross-border considerations are there?

Please see question 9.1 above as many of these liability categories are analogues in ex-U.S. territories. Jurisdictional issues may arise due to the digital nature of the industry, but other more established liability categories (e.g., tort laws) will generally be applicable in various countries for which business is conducted.

10 General

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

As discussed herein and previously, digital health (regardless of whether it is cloud-based), bring several potential legal issues related to, for example, data use, data rights, data security/cybersecurity (e.g., hacking, loss, breaches), data loss, and personal health information. These issues can arise in the U.S., in several U.S. states, and internationally as well. Cloud use can also bring forth issues depending on data location, which can be in various places around the world depending on entity location, customer location, and so on.

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

As discussed previously, digital health is a convergence of typically disparate industries: tech; and healthcare. Each industry encounters issues unique to their industry. The extremely highly regulated and appropriately risk-averse nature of healthcare can lead non-healthcare companies to have strategic (often legal) "blind spots" based on their experience leading up to the digital health endeavour. For example, non-healthcare companies, unlike healthcare companies, have not typically had to contemplate various legal issues. These can include, for example, FDA, HIPAA/HITECH, state health data laws, international health data laws, reimbursement, corporate practice of medicine and anti-kickback considerations.

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

As a continuation of question 10.2, not only are these various legal and strategic issues commensurate with converging two typically disparate industries, each having their own unique issues, these issues and their corresponding strategy should be sophisticatedly addressed and dealt with concurrently by a digital health venture. These issues include, primarily, intellectual property, FDA/regulatory, data use/privacy/security (including HIPAA), reimbursement, and healthcare transactions. These issues are interrelated and unless a cohesive strategy, from the off, addresses a plan for each of these issues, a potential investment target may have a "blind spot" that can significantly delay launch, diminish revenue, or slow or reduce adoption. It must be noted that each of these issues cannot always be "handled" by early-stage companies immediately at once. Rather, these issues should be considered, and a strategy developed that will be tested, executed and regularly reassessed so that each issue can be moved forward to resolution concurrently with the other issues.

Moreover, given the converging nature of digital health, investors should not assume that founders are broadly educated on all these subjects. Early diligence as to strategy is essential as there are not many serial digital health entrepreneurs given the youth of the digital health industry. This can rear its head, not only with understanding how to address the issues above, but also how to transact with partner entities (e.g., health systems and large pharmaceutical companies of typically greater experience and leverage), which can saddle new ventures with contract terms that affect future growth potential.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

There are two spectrums to the hurdles affecting widespread clinical adoption. On the one hand, the industry of digital health is young from an adoption standpoint. Many patients, particularly the elderly, have extensive experience and likely comfort with in-person treatment. Moreover, the parties involved in deciding on a digital health solution are very likely new to the industry as well, making robust diligence difficult to achieve on potential digital health solutions. On the other hand, due in part to COVID-19, digital health entrants have increased dramatically in the last two years. As a result, digital health consumers, already ramping up their knowledge in this space, now have to deal with a wealth of options. Which to choose? How do I navigate all these potential solutions?

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

With the dramatic increase in digital health solutions entering the market, and the aforementioned diligence shortfalls that can accompany customers, formal endorsements are one way of differentiating your solution from your competitors. Add to that the difficult financial situation in the U.S., one that may continue for a substantial period of time. Customers will be even more circumspect in analysing solutions, and may look for any designation that can mitigate the risk of purchasing a subpar solution.

Key digital health-related certification bodies in the U.S. include: American College of Radiology; American Board of Medical Specialties; American Medical Association; and the American Board of Professional Psychology.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

From a U.S. industry standpoint, payors continue to observe inconsistency in regard to the reimbursement of digital health-related therapies and treatments. Further, from a government payor programme perspective, government review of proposed regulations continues in an effort to ascertain how best to determine if a particular digital health-related device is clinically beneficial to or reasonable and necessary for a government healthcare programme beneficiary. The result is that healthcare providers seeking reimbursement for digital health-based care must utilise the coverage, coding and billing requirements of the respective payor programmes (whether government- or private-based) that are currently available and that vary by payor programme. Providers seeking reimbursement must also comply with the respective enrolment, registration and licensing requirements of such payors as they would with any healthcare treatment reimbursement submission.

Acknowledgment

The authors would like to thank Randy Peak of Haynes Boone, LLP for his efforts and input in the writing of this chapter. Randy is a Partner in Haynes Boone's Dallas office and Co-Chair of the Healthcare and Life Sciences Practice Group. He also supports the firm's Pharmaceuticals and Precision Medicine and Digital Health groups.

Randy has served as a practical and strategic legal advisor in the healthcare, life sciences and technology sectors for decades, leveraging his extensive industry background and multidisciplinary experience as he represents clients ranging from multinational Fortune 100 enterprises to start-ups on a broad range of healthcare regulatory compliance and transactional matters. He routinely counsels clients on matters relating to fraud and abuse prohibitions, healthcare privacy, telemedicine, revenue cycle management, healthcare-related licensing, outsourcing, strategic affiliations, and compliance with state corporate practice of medicine laws. Randy's healthcare industry experience also includes serving as general counsel for a nationally recognised independent academic health system and deputy general counsel for one of the country's largest healthcare supply chains, clinical consulting, and technology services organisations. In the technology sector, Randy's in-house experience includes representing a global provider of software and technology where he negotiated numerous multi-million-dollar commercial technology transactions worldwide.

Tel: +1 214 651 5000 / Email: randy.peak@haynesboone.com

Roger Kuan is a Partner at Norton Rose Fulbright and US head of the Precision Medicine and Digital Health Practice Group, where he counsels companies that are uniquely positioned in the convergence of the life/medical sciences and technology industries on how to successfully navigate the complexities of the intellectual property (IP), data rights and regulatory challenges they encounter.
Roger has extensive experience in IP strategy and portfolio management (utility/design patents, trademarks, copyrights, and trade dress), data rights strategy, licensing and technology transactions, freedom-to-operate clearances, enforcement, monetisation, IP due diligence, and dispute resolution. His practice is focused in the life sciences sector (e.g., research tools, analytical instrumentation/software, digital therapeutics, medical devices, diagnostics, biomanufacturing equipment, etc.) with an emphasis in emerging technologies such as precision medicine (e.g., genomic sequencing platforms, AI/ML, computational genomics/bioinformatics, molecular diagnostics, companion diagnostics, etc.), digital health (e.g., mobile apps, clinical decision support, software, AI/ML imaging diagnostics, wearables, etc.) and 3D printing/bioprinting.

Norton Rose Fulbright
555 California Street
Suite 3300
San Francisco, 94104
California
USA

Tel: +1 628 231 6800
Email: roger.kuan@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

Jason Novak is a Partner in Norton Rose Fulbright's Precision Medicine and Digital Health Practice Group, where he focuses on advising entities, both large and small, on the various legal issues that can arise with emerging technologies in the healthcare and life sciences industries. Tech and biotech are traditionally disparate technologies that, when blended together to form many of our most exciting new technologies, bring forth a combination of unique and interrelated legal issues. Jason has extensive experience in IP strategy and patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in and out-licensing, freedom-to-operate, various types of due diligence, IP training, risk recognition and management, and dispute resolution. Prior to starting this practice, Jason was an IP Director for Thermo Fisher Scientific, where he managed worldwide IP needs in genetic sciences instrumentation and software.

Norton Rose Fulbright
555 California Street
Suite 3300
San Francisco, 94104
California
USA

Tel: +1 628 231 6800
Email: jason.novak@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

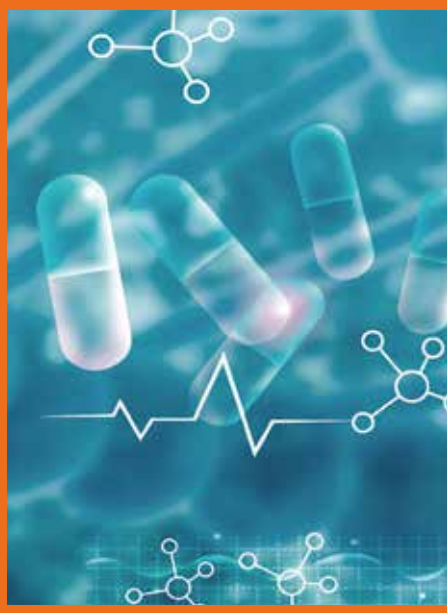
Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3500+ lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

Recognised for our industry focus, we are strong across all the key industry sectors: financial institutions; energy, infrastructure and resources; transport; technology; life sciences and healthcare; and consumer markets. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT

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 Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
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
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group