Artificial Intelligence in the Healthcare Industry

By Nasim Bazari, Legal Counsel, Middle East and Africa, and Country Legal Representative, Iran, and Ioana Ratescu, Senior Legal Counsel, Novartis Pharma AG

January 21, 2022

Key Highlights:

- Artificial Intelligence is increasingly used in healthcare.
- Regulators in several countries have developed guidance regarding AI.
- Intellectual Property Rights need to be carefully addressed.
- The use of AI raises questions regarding liability.

The Growing Use of AI Tools in Healthcare

The use of artificial intelligence ("AI") is revolutionizing several industries, not least, the healthcare industry. Catalyzing access to healthcare, supporting earlier and/or faster diagnoses, and enhancing the patient experience and outcomes, are all objectives that AI solutions have helped achieve.

But what exactly do we mean by AI? Artificial intelligence, as opposed to natural intelligence, is **the simulation by machines of processes that have traditionally required human intelligence**. It is a broad definition that covers many sub-types of artificial intelligence, such as natural language processing, image analysis, and predictive analytics based on machine learning.

Examples of the use of AI in healthcare are varied in type and objective. AI can be used to innovate across research and development, to optimize business processes, and to engage with external stakeholders. Some AI tools are not relied on for diagnosis but instead are used for diagnostic support, meaning that the treating physician uses the tool's result as guidance rather than as a diagnosis.

As noted by Angela Spatharou, Solveigh Hieronimus, and Jonathan Jenkins in "Transforming Healthcare with AI: The impact on the workforce and organizations" published by KcKinsey & Company, examples of AI enabled tools range "from apps that help patients manage their care themselves, to online symptom checkers and e-triage AI tools, to virtual agents that can carry out tasks in hospitals, to a bionic pancreas to help patients with diabetes."

Another example is an algorithm that is taught by expert radiologists to recognize key biomarkers on scans and identify abnormalities. These are known as AI expert systems. You may wonder why such a tool would be needed if it is to be trained by experts that already exist. The reason for this is that for many patients across the globe, physical access to expert radiologists is not possible, due to lack of local expertise or a concentration of expertise in cities that are distant from rural locations.

As a result, the AI tool could enhance performance and potentially reduce time to diagnosis by "downloading" this expertise and delivering it to locations that otherwise would not have had access to it. Even in cases where access to experts is not an issue, such processes are much faster when using an AI tool as compared to a human.

Empowering healthcare systems with AI is at the top of the agenda for many healthcare providers, governments, investors, and innovators. Governments in various countries actively focus on the use of AI in healthcare, such as Finland, Germany, the United Kingdom, Israel, the UAE, China, and the United States. The recent pandemic has increased the focus on the use of digital technology in healthcare, and the need to create legislative frameworks for the use of such technology.

The Legislative Landscape of AI (EU, US)

The European Commission has been the first to propose a legal framework on AI in the European Union ("EU"). The Proposal for an AI Regulation ("AIA") published on 21 April 2021 sets out plans for a comprehensive EU regulatory framework that has the potential to set a global standard for the regulation of AI.

AIA uses a broad definition of AI systems which could also encompass systems leveraging logic-based decisions or retained information. It lays down a layered risk-based approach, with AI posing unacceptable risk being outright prohibited, while high-risk AI will bear the bulk of regulatory requirements. Low-risk AI will only be subject to limited transparency obligations.

Regulators in various jurisdictions beyond the borders of the EU have also been developing proposals and guidance designed to tackle these emerging challenges in recent years. For example, the US Food and Drug Administration ("FDA") published a discussion paper in 2019 entitled Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning-Based Software as a Medical Device. More recently, the FDA published its action plan on furthering AI in medical devices in January 2021. However, currently there is no expectation that the US would issue any US specific federal guidance on AI.

AI and Ethics (transparency, integrity, bias, privacy, sustainability)

It is part of in-house counsel's role in a business to keep abreast of the legal and regulatory changes that may impact the business or industry. In-house counsel may need to go above and beyond, such as regarding the case of the use of AI in the healthcare industry, where regulation is evolving so rapidly that we need to be agile and at times pre-empt the issues or ethical considerations that could arise.

In addition to the external regulations mentioned above, **internal frameworks are essential** to ensure that organizations are leveraging AI in an ethical manner. The input of an in-house lawyer is essential to create an internal ethical framework that guides associates on acceptable uses of AI, in close collaboration with other functions such as data & digital function(s), and compliance.

The pharmaceutical industry has been publishing ethical frameworks for the responsible use of AI. For example, Novartis' commitment is to deploy AI systems in a transparent and responsible way, to ensure "that the use of AI systems has a clear purpose, that is respectful of human rights, and is accurate, truthful, not misleading, and appropriate for their intended context." (https://www.novartis.com/about/strategy/data-and-digital/artificial-int…)

Companies should provide customers and clients with "meaningful information about the logic involved" in any automated decision taken by an AI algorithm relating to their care, which can be challenging where these decisions rely on sophisticated and dynamic AI models.

Transparency is key. The tool must be transparent to allow appropriate accountability. To ensure transparency, the foundations must be strong. This includes a robust governance over the design and use of AI, with the appropriate ideation including risk assessment, validation, and monitoring of a solution. For example, important questions include:

- Is the data reliable?
- Is the patient or healthcare professional aware that they are interacting with AI, and what data it is collecting – has the third party provided an informed consent?
- Is the tool's methodology traceable and auditable?

Data

Many deep learning AI models are trained on vast datasets that must be carefully identified and labelled to train the algorithm before it is useable. Often, collaborations are between a party with data and a counterparty with a model; the two parties join to develop a model useful for performing a given task. Data is generally not very fungible or substitutable in order to achieve a particular outcome, while the algorithm or model is much more fungible or substitutable. Therefore, **ownership and usage rights of data** need to be carefully addressed in any collaboration.

An AI algorithm is only as good as the datasets from which it learns. The datasets on which it is based may come from multiple sources and could include both personal and non-personal data.

Quality Data

The quality and selection of data from each of these sources are critical to the success of an AI solution. The dataset should be **unbiased, accurate and representative of the studied population**.

This is to eliminate or prevent potential risk of unintended discriminatory decisions concluded from the AI model, which may possibly lead to unfair outcomes, or more significant issues concerning safety, security, entitlement, or healthcare.

To ensure quality datasets are used, it is important for organizations to invest effort in knowing:

- Where the data has originated from,
- How it was collected,
- Its completeness,
- How it was curated and moved within the organization,
- How its accuracy is continuously maintained over time, as well as
- Whether the datasets have been subject to human interventions.

Legitimate Sources

In addition to the ethical considerations surrounding datasets, it is important to also consider whether the datasets come from **legitimate sources conforming to legal requirement and/or contractual rights and obligations**.

It is imperative to map the process of an AI solution to check where, how, by whom and for what purpose the data is collected, processed, and stored. Data must only be obtained and used for an informed legitimate reason; its security, integrity and quality should be maintained, and it should only be retained for as long as is necessary.

All these items, including the ownership of the data, **should be clear in the legal agreement** and should be in compliance with the applicable data privacy regulations, such as by being GDPR compliant if the data falls within the scope of EU General Data Protection Regulation or abiding by HIPAA rules in the US.

In some jurisdictions there are geographical limitations to the movement of health data which should be adhered to due to pressing issues regarding country public health and / or national security. This limitation may be in force through data protection law or any other country law (such as a Health Data Law). Advice from a local lawyer and data privacy lawyer is a must when considering AI solutions.

AI in SaMD

Software as a Medical Device ("SaMD") is software that is intended to be used for specific medical purpose(s) as specified in the definition of medical device under the EU Medical Devices Regulation 2017/745 ("MDR").

To qualify as SaMD, the software must process patient-specific input data to generate a patient-specific data output. According to the guidance from the UK's Medicines & Healthcare products Regulatory Agency's "the monitoring of general fitness, general health and general wellbeing is not usually considered to be a medical purpose."

Moreover, according to the same guidance, software that is intended to indicate the risk that a broad group of the population has of developing a disease is unlikely to be a medical device; however, according to guidance endorsed by the Medical Device Coordination Group, drug planning systems (e.g. chemotherapy) that are intended to calculate the drug dosage to be administered to a specific patient are qualified as medical devices.

The European Commission had already announced in its White Paper on Artificial Intelligence that EU product legislation would be impacted by AIA and mentioned the MDR specifically in that context.

All software that qualifies as a medical device under the MDR or medical devices running software with an AI component will be classified as high-risk AI systems under AIA because it is "the product whose safety component is the AI system, or the AI system itself as a product" covered by the MDR. SaMD could also fall under this scope and this would cause duplication of regulatory requirements for AI products with MDR, as warned by the European Association for Medical Devices of Notified Bodies (TEAM-NB) in their position paper.

AIA sets up a **system of conformity assessment for AI systems**, which, will almost always double the assessment as a medical device under the MDR if the systems are deployed for medical intended purpose(s). The conformity assessment will also involve notified bodies similar to the MDR. Some measures were indeed prescribed to avoid the overlap, such as the possibility to provide a single set of technical documentation for the AI systems that are also devices in the meaning of the MDR, however, there remains abundant overlap which is not yet addressed by AIA.

Development Challenges & Regulatory Constraints regarding SaMD

In an increasingly dynamic and innovative market for digital health solutions, the development and use of SaMD has already served to challenge and disrupt existing regulatory frameworks. To this, AIA added questions of how SaMD is to be regulated when AI algorithms also form a part of its programming. This requires an understanding of some of the unique challenges that AI can give rise to in the context of SaMD.

Under MDR, software devices must be "designed in a manner that ensures repeatability, reliability and performance in line with their intended use" (MDR Article 17.1) However, as noted by the law firm Mason Hayes & Curran in "AI in Medical Devices: Key Challenges and Global Responses," it is more difficult to meet these requirements with AI than with conventional software algorithms, because instead of being programmed "line by line" "many AI applications […] are trained and tested using large data sets," which "makes them difficult to validate and verify using existing standards."

Another substantial development challenge is the ‘black box’ issue. As noted by Mason Hayes & Curran, the complexity of the billions of calculations performed by a sophisticated neural network to reach a decision or result “makes it very difficult to trace or diagnose the source of incorrect results in a meaningful way.”

Post-marketing, the provider of an AI system will also have regulatory obligations to proactively monitor, collect and review experience gained from the use of AI systems for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions, similar to post-market surveillance under the MDR.

Finally, there are also significant challenges for medical devices competent authorities, who will have to act as market surveillance authorities for AIA. This would trigger additional regulatory constraints for EU Member States’ competent authorities which would have to gather the expertise in AI needed for proper market surveillance and enforcement, in addition to the much-needed knowledge of medical devices.

Ownership of SaMD

When developing an AI algorithm, intellectual property rights (“IPR”) are a critical issue. There are several types of IPR, including patents, copyright, and trademarks.

It is imperative to ensure that, as part of the contractual discussions, a well-drafted IPR definition is agreed, including all of the rights that would arise from the new launch. The definition of IPR would be used in the IPR clause (at a minimum), which would set out key terms such as:

- any warranties and representations about the IPR such as that it does not infringe on any third party’s IPR,
- which of the parties owns which right and who is responsible for registering it,
- which of the parties has a license to which right (if any), and
- whether the non-owning party has the right to step in and take over an IPR in the event that the owning party does not upkeep or commercialize the IPR.

Copyright

One of the basic principles of the Berne Convention is that of **“automatic protection”**, which means that copyright protection exists automatically from the time a qualifying work is fixed in a tangible medium.

Copyright covering algorithms can only be applied **once the programmer converts the algorithm into source code**; the software underlying machine learning is generally protected by copyright laws, and trained models are able to be protected by copyright, but, as noted by the US Copyright Office, **“protection does not extend to functional aspects such as algorithms, formatting, logic, or system design”**.

There are several stages in the process where infringing copies of an original work (or “Works”) may be made, including when Works are input to teach the machine (training datasets), how and from where the foundational materials are obtained, and when the training datasets are copied and stored and when the tool's results contain a substantial part of the training datasets.

Patents and Trademarks

On the other hand, **patents and trademarks need to be registered**. In general, as set out by the World Intellectual Property Organization, a patent is only granted if there is a "new way of doing something, or a new technical solution to a problem".

For a patent to be granted, technical information about the invention must be disclosed to the public in a patent application, which would then be available to be utilized or commercialized by others when the patent expires – this is the benefit of patents to the non-patentor. It is advisable to consult with an IP attorney and, ahead of this consultation, ascertain the business's appetite for ownership of IPR.

Trade Secrets

An alternative to patent protection is that of trade secrets. To qualify as a trade secret, the information protected by this IPR must have economic value and be kept confidential by the company, such as through legal agreements, physical or virtual segregation of the information, and by taking action against those who disclose the information.

The core difference between a patent and a trade secret is that of disclosure. To obtain patent protection one must disclose the invention (and meet the patentability criteria), which would mean that after the patent has expired, typically 20 years after grant, the detailed submission made to patent authorities for the patent to be granted would now be information that could be publicly used. Consider seeking legal advice on the patentability of an algorithm – a bar which algorithms do not always reach - in comparison to how to maintain it a trade secret.

Virtually all software nowadays is developed using open-source code, and such **open-source code may carry with it license restrictions** which are not always optimal. Therefore, it is important to **understand the sources of code used** to develop algorithms and models and be aware of the licenses associated with such code and to **consider indemnity provisions** related to third-party claims.

Liability and risk allocation

Characteristics and complexities of AI systems and their applications make it more difficult to ensure compensation. Existing liability regimes ensure basic protection for victims from operation of AI, and few countries have a liability framework specific to AI and other emerging technologies. One exception is in the UK, where the Automated and Electric Vehicles Act 2018 prescribes that liability for damage caused by the insured person's automated vehicle when driving itself lies with the insurer.

Many countries in the EU have product liability laws, which basically state that if the product is defective, a claim can be made against the manufacturer or the supplier. However, there is uncertainty in relation to the classification of software whether it qualifies as a product or service, and in which laws liability for these products currently lies.

Liability could be claimed in tort or negligence. However, negligence requires a duty of care and an activity or a behaviour that is outside of reasonable behaviour. When is reliance on AI or non-reliance on AI considered to be reasonable?

Liability in contract is defined in the contractual terms which set out the requirements for the manufacturer or supplier. If terms are breached, then a contractual claim can be raised. But contracts need to be carefully drafted by lawyers with a clear understanding of the functioning of the AI system.

The EU has set out recommendations regarding liability. It proposes strict liability for the person who exercises a degree of control over the risks connected with the operation and functioning of the AI system and benefits from its operations. Systems should have a logging by design which would track what actually happened to make sure one could go back and check where the problem arose.

Conclusion

Research and development of AI applications for the healthcare sector continues to gather pace internationally. In tandem, more and more medical devices incorporating AI are arriving to market. As a result, there is a pressing need for a coherent, consistent, and ultimately harmonised approach to the regulation of these powerful yet poorly understood technologies. Work to develop the required regulatory guidance is well underway and interested stakeholders should actively monitor developments in the various regions and jurisdictions in which they operate to stay abreast of this continuously evolving regulatory landscape.

It is hoped that growing awareness around the risks and challenges presented by the use of AI in healthcare, as well as the policies being developed to manage those risks, can also continue to foster increased credibility and public trust in these technologies, which are set to shape the provision of healthcare for years to come.

All opinions expressed by the authors are personal perspectives and do not reflect the opinions of Novartis, its affiliates, or employees. The content herein is not intended to be a substitute for professional medical or legal advice and is for informational purposes only.

Learn More:

- “Top Ten Issues on Liability and Regulation of Artificial Intelligence (AI) Systems” by Tarek Nakkach, ACC Resource Library, August 2, 2021

- "Artificial Intelligence and Regulatory Compliance", by Emily Foges, Emma Walton, ACC Docket, January 2, 2020

- "Global Legal Insights: AI, Machine Learning & Big Data 2020, 2nd Edition" by Global Legal Group

- Join the ACC IT, Privacy, and eCommerce Network and Health Law Network (ACC members only)

- Search the ACC Resource Library

Not a member? Join ACC Today!

Disclaimer: The information in this resource (or in any resource collected in ACC's virtual library) should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered as representing the views of its authors, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers. For legal advice or representation, please engage a legal counsel.