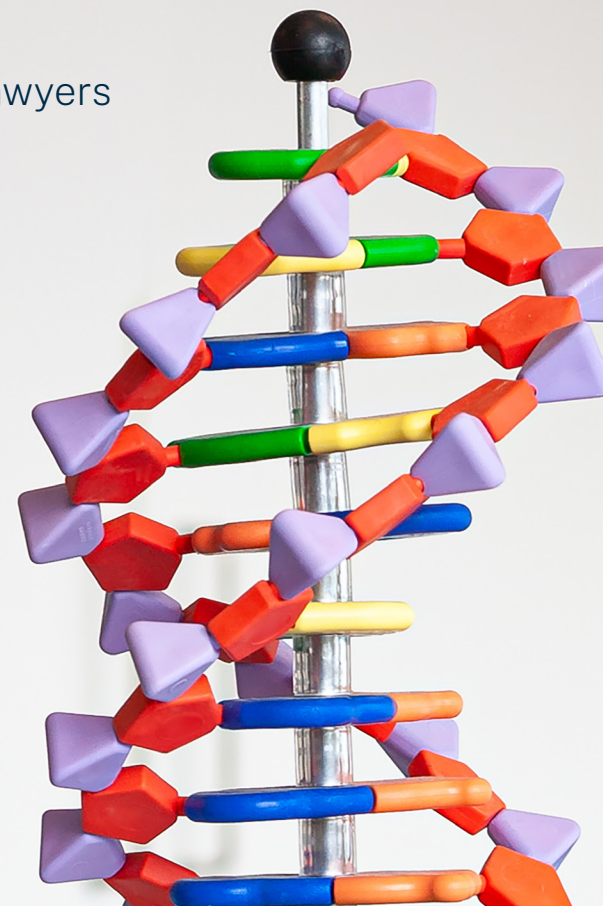
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Digital Healthcare 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Contributing Editor
William Tanenbaum
Moses & Singer LLP



Chambers

Global Practice Guides

Digital Healthcare

Contributing Editor

William Tanenbaum

Moses & Singer LLP

2023

Chambers Global Practice Guides

For more than 20 years, Chambers Global Guides have ranked lawyers and law firms across the world. Chambers now offer clients a new series of Global Practice Guides, which contain practical guidance on doing legal business in key jurisdictions. We use our knowledge of the world's best lawyers to select leading law firms in each jurisdiction to write the 'Law & Practice' sections. In addition, the 'Trends & Developments' sections analyse trends and developments in local legal markets.

GPG Director Katie Burrington
Content Management Director Claire Oxborrow
Content Manager Jonathan Mendelowitz
Senior Content Reviewer Sally McGonigal, Ethne Withers
Content Reviewers Vivienne Button, Lawrence Garrett, Sean Marshall, Marianne Page, Heather Palomino, Deborah Sinclair, Stephen Dinkeldein and Adrian Ciechacki
Content Coordination Manager Nancy Laidler
Senior Content Coordinator Carla Cagnina
Content Coordinator Delicia Tasinda and Hannah McDowell
Head of Production Jasper John
Production Coordinator Genevieve Sibayan

Published by
Chambers and Partners
165 Fleet Street
London
EC4A 2AE
Tel +44 20 7606 8844
Fax +44 20 7831 5662
Web www.chambers.com

CONTENTS

INTRODUCTION

Contributed by: William Tanenbaum, **Moses & Singer LLP**

Moses & Singer LLP is a New York firm recognised in the United States and internationally for the strength of its healthcare practice. It assists companies entering the US market with navigating the issues arising at the intersection of regulatory compliance, intellectual property law and the special features of the US healthcare system. Lawyers in the firm's digital healthcare practice have worked as lawyers at government healthcare agencies, served as lawyers at academic hospitals, and have leadership roles in the digital healthcare associations. The firm's dedicated Data Law group provides a broad-gauge, multidisciplinary practice to guide clients in leveraging their data assets as new technology and analytics platforms create new business opportunities, including in digital healthcare. This includes structuring, drafting and negotiating joint ventures and agreements in the US style. Its lawyers are ranked in the US and Global editions of Chambers.

Contributing Editor

William Tanenbaum is a partner in the technology, healthcare, IP, and data law practices at Moses & Singer in New York. He assists law firms in representing clients entering the US healthcare market and structuring partnerships with US companies and hospitals and complying with US IP and regulatory regimes. Bill is a past President of the International Technology Law Association. Chambers notes that his "technology approach and understanding of healthcare – his domain of expertise – is a winning combination".

Moses & Singer LLP

The Chrysler Building
405 Lexington Avenue
New York
NY 10174
USA

Tel: +1 212 554 7800
Fax: +1 212 554 7700
Email: wtanenbaum@mosessinger.com
Web: www.mosessinger.com

INTRODUCTION

Contributed by: William Tanenbaum, **Moses & Singer LLP**

Introduction

In the near future, "digital healthcare" will become just "healthcare" as data and digital healthcare technologies and practices are integrated into most fields of patient care and medical research. Data, AI and the internet of medical things (IoMT) are critical to the power and efficacy of digital healthcare, and accelerating advances in them require accelerated innovation in structuring and drafting healthcare technology and data agreements.

New forms of agreements that address the issues of data, AI and the IoMT are necessary to implement advances in digital healthcare.

Data, AI and Machine Learning

Data and actionable insights

Data becomes valuable in healthcare when it is converted into information, and information becomes valuable when it is converted into actionable insights. These insights are what lead to advances in clinical medicine and research.

Data does not manage itself

Data is not technology and data does not manage itself. Data must be collected, transmitted and analysed using digital healthcare technologies. Medical devices that are connected together in computer networks constitute the IoMT. These connected devices collect data from multiple sources and provide it for multiple purposes, including use in AI, to generate insights that can be acted upon.

AI is not a single technology

AI is not a single technology but a series of technologies. These include algorithms, which are a set of instructions that tells a computer how to process data.

Machine learning and "augmented" intelligence

Machine learning is a form of AI in which one or more algorithms process data without having to rely on rules that are programmed into the algorithm. Algorithms are developed by human programmers, but increasingly AI refines and generates new algorithms without direct human involvement. Machine learning uses data to train the algorithms to identify patterns in the data and generate correlations and predictions, such as whether a spot on a medical image is a tumour and whether the tumour is benign or cancerous. The algorithm assigns weight to different factors in reaching its "conclusion" that a tumour is, or is not, benign.

Because the weight assigned by machine learning is part of the so-called "black box" of AI, physicians need to know what weight was assigned to different factors in order to trust the outcome and use it in patient care. As a result, AI in healthcare is "augmented intelligence" rather than "artificial intelligence" because it is machine learning in combination with doctors' skills that create the healthcare benefit.

AI and the IoMT do more than collect data. They also generate new data, which in turn further trains the algorithms. Moreover, the collection, creation and use of data and machine learning complicate the application of IP law to data in particular and to digital health technologies in general. Accordingly, contracts should be used to bring more clarity to the allocation of ownership, licensing and sharing rights in data and machine learning outputs. Such contractual allocation is important in the multi-technology, multi-vendor, multi-user, multi-stakeholder environment that characterises both hospitals' healthcare systems, healthcare institutions and

Contributed by: William Tanenbaum, **Moses & Singer LLP**

healthcare providers (henceforth "hospitals") and their technology and data providers.

Most digital healthcare agreements are combined data, technology and IP agreements subject to various healthcare, data protection, privacy and other regulations. The regulatory overlay adds complexity to contract negotiations when different jurisdictional requirements apply to hospitals and/or their providers.

The impact of COVID-19 on digital healthcare technology use

COVID-19 has accelerated the development and deployment of digital healthcare technologies (including the use of telehealth and remote medicine), and in many cases made existing agreements inadequate for digital health. COVID-19 has increased the opportunities for technology vendors to provide upgraded digital health technologies to hospitals and regulations have changed to remove obstacles to the use of digital healthcare technologies for telehealth services.

IT infrastructure

Most current hospital IT systems are not designed to handle the volume of data now generated by the IoMT, including networks formed by connecting multiple IoMT subnetworks, or to conduct the sophisticated data analytics made possible by advances in AI technology. As a result, the use of digital healthcare technology requires the upgrading of IT infrastructures and negotiating the agreements that provide for those upgrades, which often involve moving to cloud computing and data storage environments with their attendant security risks. Here legal departments and outside counsel must co-ordinate with the hospital IT and medical departments. Similarly, technology vendors must ensure a fair allocation of rights and responsibilities when they contribute to parts of the overall technology infrastructure.

AI as a change agent

To use AI as a change agent to improve healthcare, a hospital's chief digital medicine officers and other data professionals must work together with IT departments to implement the desired transformation in data analytics and use of the IoMT. This is another example of the need to upgrade IT infrastructures. In addition, successful use of AI as a change agent requires the involvement of a hospital's legal compliance officers. In designing new data management systems, it is easier to build-in regulatory compliance than to retrofit it.

Connected Devices

Examples of connected devices in healthcare are wearables (eg, sensors and data collection devices attached to the skin), implantables (eg, pacemakers), ingestibles (eg, diagnostic pills that transmit images), smartphones and similar devices, real-time location sensors (for hospital staff and medical equipment) and virtual reality and augmented reality devices (which are used in surgery and medical student training). Even drones, used in the healthcare aspects of disasters, and devices that transmit medical images and data between ambulances and emergency rooms are part of the system of connected devices.

5G Wireless Networks

The advent of 5G networks will add power to digital healthcare technology and bring advances in patient treatment. 5G networks are fifth-generation wireless networks that will replace the current 4G (fourth generation) networks and bring significantly greater speed, greater bandwidth and reduced latency, all of which means

Contributed by: William Tanenbaum, **Moses & Singer LLP**

that more and richer data can be transferred in the same amount of time.

Connected devices create volumes of data that 5G can transmit between devices and the hospital's general IT systems. As a result, connected devices in the IoMT will receive data more quickly and process it faster for increased functionality of machine learning.

Telehealth is an area where 5G can improve patient care by delivering newly created medical images to a physician's desk during patent visits, allowing remote treatment by specialists located in distant medical centres, reducing the need for seriously ill patients to travel and providing medical care to rural and inner-city areas. 5G-enabled telehealth can be used within hospitals to connect emergency rooms with specialists and allow doctors at the main location of a hospital system to connect with doctors and patients at other facilities in the same system.

Preventative Healthcare

The types of connected devices in the IoMT include:

- physical healthcare devices subject to regulatory approval (such as by the Food and Drug Administration (FDA) in the United States);
- software as a medical device (SaMD), which essentially constitutes virtual machines, also subject to FDA approval;
- devices that collect, store and transmit health data in digital form, where the data is subject to healthcare regulatory schemes as well as privacy laws (including pursuant to the Health Insurance Portability and Accountability Act (HIPAA) in the United States); and
- wellness and fitness devices that are not subject to FDA or similar regulatory approval and that can transmit data without being subject to HIPAA and other healthcare data protection regimes (although privacy laws of general applicability may apply).

The combination of data from these devices combines traditional patient data with wellness data that creates rich data sets and enables a growth in preventative healthcare, which is distinguished from medical interventions such as surgery.

Preventative healthcare also requires updated technology and data agreements in order to collect, generate and share data from medical and non-medical devices from different sources and for the use of data for overlapping purposes.

The "Solid" Internet Protocol and Individual Control of Personal Health and Wellness Data

The combination of health and wellness data will lead to a demand for individuals to have greater control over how this data is used and for what purposes. This includes the ability of individuals to monetise their data by providing it to various institutions for a range of research, product development, data analytics and other purposes. A means to accomplish this is provided by the "Solid" protocol, which stands for "socially linked data".

Solid has been developed by Sir Tim Berners-Lee, the inventor of the World Wide Web, in collaboration with the Massachusetts Institute of Technology. It is a Web 3.0 "web decentralisation project" designed to give individuals more control over which persons and things access and use their data; "things" refers to the applications on the internet. In this sense, Solid is designed to provide more individual control than exists in the current World Wide Web where individuals

Contributed by: William Tanenbaum, **Moses & Singer LLP**

have limited control over how their data can be collected and used.

Solid makes use of "pods" (personal online data storage), which are storage areas controlled by individuals and which function as secure, personal web servers for data. Each pod has access rules that are specific to it. Individuals have the right to grant or revoke access to data in their pods (an individual can have more than one pod). Any person or application that accesses data in a pod uses a unique ID. Solid's access control system uses these IDs to check whether an entity or internet application has the right to access and use data in the pod.

The connection between AI and Solid is that an individual can use AI to determine which data to load into the pod. The individual controls the machine learning algorithm and can change algorithms and thus the data loaded into the pod. The algorithm can be trained to screen for data features to be included and excluded from the pod. Because a pod controls access to and use of the data, it indirectly controls the use of a third-party AI to which the pod owner has granted use rights. Individuals can also use self-service AI to perform machine learning and data analytics on their own data and to determine whether the data set includes all or only part of health and wellness data.

From another perspective, such data analytics can guide individuals in deciding which data to include in their pod, or if they have more than one pod, to decide which data to include in each pod. Each pod can in turn operate according to separate rules for access and use of data sets by third parties and by "things" such as software programs.

A Proposed Licensing Paradigm: "Decision Rights"

At a technology company and healthcare institutional level, sharing data requires licences. As a practical matter, it is often difficult for parties to a transaction to reach an agreement on ownership of data because the scope of ownership and its status under IP rights is unclear under the present state of the law. A party is often concerned that by assigning ownership rights it will be giving up rights it may need in the future. Accordingly, parties focus on sharing data and the scope of use rights under sharing arrangements.

If we shift the focus from ownership to data use – because that is often the real issue involved – then we need a legal framework to govern the scope of use and sharing with particularity, in order to protect both providers and users of data sets.

This article proposes "Decision Rights" as that legal framework. Decision Rights is a licensing model that defines the purpose of conducting analytics and the use of the results in terms of decisions that can be made based on them. The model also provides the entity controlling the data with a mechanism to grant (and enforce) rights in the same data to different users for different purposes, thus enhancing data monetisation and revenue generation. Decision Rights protect against regulatory sanctions by putting boundaries on the data use that constrain the use rights on downstream parties. Under a Decision Rights framework, those entities owning or controlling a database would grant a set of rights defined by the decisions that can be made and, if desired, limit the rights to a business unit or even specific individual.

INTRODUCTION

Contributed by: William Tanenbaum, **Moses & Singer LLP**

Addressing Cybersecurity Risks in Connected Devices

The IoMT gives rise to cybersecurity risks on various levels:

- the level of the device itself;
- when the device is connected into an IoMT;
- the connection of different IoMT networks to each other; and
- the connection of the IoMT networks to the hospital's main computer systems and its IT infrastructure generally.

These risks have led the FDA to issue regulatory guidance in its "Cybersecurity in Medical Devices: Quality Systems Considerations and Content of Premarket Submissions". The FDA issued this guidance in April 2022. This was not a set of formal regulations but guidance that the FDA provides to medical device manufacturers to meet in submitting devices for regulatory approval (ie, premarket submissions to the FDA). The background for this guidance is based on the following factors: (i) the very sophistication of advanced medical devices results in an increased risk to the safety and effectiveness of the device; and (ii) past cyberattacks have in fact rendered medical devices and hospital networks inoperable and disrupted the delivery of patient care.

The FDA guidance addresses these risks by requiring device manufacturers to adopt "security by design" (as an analogue to "privacy by design") and to incorporate cybersecurity measures in the design and manufacture of medical devices. The guidance provides details on how the FDA will approach whether or not to approve the security of a medical device. It assumes that cybersecurity vulnerabilities exist now and that new threats will arise in the future. It therefore requires that manufacturers plan for future threats by having plans in place to mitigate risks that will arise, even if the exact nature is not yet known. The cybersecurity guidance focuses on the following areas, among others.

Security Risk Management

Security risk management includes threat modelling, or a process to identify security objectives, risks and vulnerabilities. This applies not only to the device itself but to the system in which it operates (including the applicable IoMT). Manufacturers are to define their countermeasures to prevent or mitigate the effects of threats during the device's life cycle. The approach assumes "zero trust" (ie, that an adversary already controls the relevant IoMT). The guidance also requires the publication of a "Software Bill of Materials" (SBOM). The SBOM is to identify the components that are provided by the manufacturer itself and the components that originate with specific third parties. These are both hardware and software components (including open-source software). The SBOM must also identify which are the dependences of different components upon other components. While this is to allow hospitals to identify and assess the vulnerabilities of the components and their combination, it can also be viewed in some respects as shifting of vulnerability assessments to the hospitals.

Security risk easements of uncured defects must be identified to the FDA when the device is submitted for approval. A total product life cycle approach is required. There is to be a continuous refresh of security risk management activities to ensure timely identification of security risks and their mitigation.

Security architecture

Security architecture requirements include a set of security controls in specified categories including programming code integrity, security event detection, cryptography and "patchability"; ie, how software vulnerabilities will be remediated by patching the software on an ongoing basis. Security architecture assessments are to be made at the system or network level with a focus on both internal and external interfaces. Overall, the guidance is intended to ensure that manufacturers design devices to be capable of addressing future security threats that may arise.

Cybersecurity testing

Four types of security testing are to be conducted on medical devices during design verification and design validation stages. These are:

- security requirements;
- effectiveness of threat mitigation;
- vulnerability testing; and
- penetration testing.

Buying Technology to Build Technology

Risks resulting from changes in components in a device

Technology companies that build medical devices in particular and digital healthcare products in general need to buy technology in order to build their own technology. Digital healthcare products and services often consist of hardware components, software, services and raw materials provided to the product manufacturer or service provider by subcontractors, business partners and other third parties. The risks that arise, especially with connected devices made part of an IoMT, are as follows.

- If a third party changes a component included in the overall device, the substituted component may result in a changed device that no longer qualifies as an approved device. Put another way, the product will have to be approved as a new product with the required expenditure of time and funds.
- A change in a third-party component may decrease the functionality of the device as a whole. This is a risk that applies whether or not the device requires regulatory approval.

A change in a component may result in a change to a device that adversely affects the performance of other devices connected to it or otherwise dependent upon it (eg, for the generation of data).

Contractual steps to address these risks

Digital healthcare technology companies can use contracts to address the risks introduced by changes in constituent components. The technology company can require approval of changes or substitutions in components of raw materials. Another solution, especially when continued regulatory approval prohibits changes in components, is to require the subcontractor to continue producing the old version of the product along with the new version. This way the technology company can be assured of a supply of conforming components.

Similarly, the technology company can require the subcontractor to produce a large quantity of the old version of the component for the company to use even as the subcontractor provides the new version to other customers. The technology company as buyer can build a substantial inventory of the required component for its use, even if the subcontractor changes the component. The contract can require the provision of this inventory when both parties know that the component will change either because of sup-

Contributed by: William Tanenbaum, **Moses & Singer LLP**

ply change problems or because of advances in technology. Finally, the technology company can secure alternative backup suppliers, which also may mitigate the dangers of supply chain problems for products manufactured in certain countries.

Backward compatibility

Another issue that digital healthcare technology companies face is ensuring that new versions of components continue to work with the prior versions of the components. To address this, the technology companies can require that subcontractors and suppliers design components to be backwards compatible with prior versions. A common approach is to require the new version to be backward compatible with the earlier two versions of the component. (Among other things, this will allow the technology to support and maintain products that it sold to customers before the new version was released.) The contract should define what backward compatibility means. It may require that the component be backward compatible with external devices that connect with the technology company's product.

Backward compatibility should include, where applicable, requirements that the new version connects with, interfaces with, integrates with and otherwise works in conjunction with the external devices and the prior versions of the component.

Forward compatibility

The success of backward compatibility is increased if each version of the component is designed to be forward compatible with planned new versions. This is implemented by technology requirements in contracts.

Cybersecurity requirements

Backward and forward compatibility are an important part of implementing "security by design". Contracts should address the risk that new versions of a component will introduce cybersecurity risks that did not exist before or that become an avenue for a cyber-attack on a hospital's IT infrastructure or an avenue to make unknown changes to data use in machine learning that, in turn, can have an adverse effect on medical care.

Virtual Assistants

Virtual assistants, such as Amazon's Alexa, will increasingly become the user interface with digital healthcare technologies as well as part of a system of connected devices, and they raise several issues. They can expose the IoMT networks to cybersecurity attacks and data breaches. They can enable unauthorised access to personal health information. Depending on the role they serve in part of a system of connected devices, they may be required to meet regulatory requirements (eg, the requirements for "Business Associate Agreements" under HIPAA under US law) when they are providing services to healthcare institutions that are under an obligation to securely store and transmit digital personal health information.

They also raise the following legal questions.

- What privacy requirements apply to communications transmitted through the virtual assistant and to conversations recorded by the device?
- How long will hospitals need to retain recordings for legal compliance purposes and for the hospital's policies for research and patient care?

Contributed by: William Tanenbaum, **Moses & Singer LLP**

- Will records be accessible by regulators and what is the permitted scope of use by regulators?
- How will recordings be used in litigation?
- What is the scope of liability of the relevant parties that can arise for unauthorised use of an IoMT or data?
- How will virtual assistants be used in training algorithms for machine learning?

Open-Source Software

Open-source software is attractive to academics. However, professors and researchers often do not understand that open source is not free software but a free licence to use the software and that licences have restrictions and provide benefits. They are often not aware that there are nine basic open-source licences and that they have different terms. Some licences can result in a loss of IP rights. Accordingly, legal departments should establish rules governing the internal and external use of open-source software with a focus on protection of intellectual property rights.

Conclusion

The IT ecosystem of AI, data and the IoMT requires contracts that provide the necessary interoperability and data exchange between connected devices and also impose technology requirements to address cybersecurity risks. This in turn requires contracts that require co-operation from the manufactures of devices and providers of services used in the IoMT. Accelerating advances in AI and data analytics and the technological capabilities of software and physical devices will improve patient care and speed up medical research. All this requires thoughtful contracts so that all technology companies and hospitals can meet opportunities and mitigate risks as digital healthcare evolves.

AUSTRALIA

Law and Practice

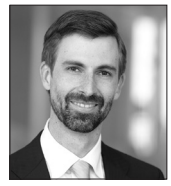
Contributed by:
Greg Williams, Timothy Webb and Ken Saurajen
Clayton Utz

Contents

Clayton Utz is recognised as a leading life sciences law firm. With 17 partners and over 25 qualified lawyers across its Sydney, Melbourne, Brisbane and Perth offices practising in this area, the firm continues to build a reputation for innovative and incisive advice. The team has a unique combination of scientific, regulatory and legal expertise in prescription pharmaceuticals, OTC and complementary medicines and medical devices, and is consistently the legal firm of choice for many Australian and global pharmaceutical and medical device companies. The firm advises on all aspects of the product life cycle, including the strategy, protection and enforcement of IP, clinical trials, marketing approval, product labelling, reimbursement, approval and registration processes, promotion and distribution, product risk, product liability and product recall. Clayton Utz counts both established global pharmaceutical companies and agile start-ups among its clients. It has advised Medicines Australia (the prescription pharmaceutical industry body) about significant policy initiatives in the pharmaceutical space.

Authors

Greg Williams has over 20 years' experience providing regulatory and litigation advice to Australian and overseas pharmaceutical and medical device companies. In the regulatory sphere, he provides advice across the whole product life cycle, including product registration, reimbursement, advertising disputes, and product safety and recalls. He has particular expertise in providing strategic advice in relation to pricing and reimbursement issues and has assisted a number of clients of Clayton Utz to navigate difficult and contentious Australian reimbursement applications. In litigation, Greg defends product liability claims and class actions. He has been involved in the defence of several prominent pharmaceutical and medical device product liability claims.



Timothy Webb is a partner in the intellectual property and technology practice group at Clayton Utz. His expertise covers all aspects of intellectual property law (eg, copyright, trade marks, patents, designs, confidential information, domain names) in both contentious and non-contentious matters. He has extensive public sector experience. He has also acted for clients in landmark Australian test cases for both copyright and designs. Tim is also the joint head of the firm's trade mark and brand protection group, which is responsible for matters relating to the registration of trade marks, including clearance.

Ken Saurajen is a partner in Clayton Utz's intellectual property and technology practice group, with a formidable reputation for the design and structuring of some of Australia's and the Asia Pacific region's most difficult and unorthodox telecommunications, media and technology transactions. He specialises in strategic, front-end information technology contracting and is renowned for his work on large-scale, complex IT procurements, outsourcing and transformation projects, software licensing, electronic payment systems, bespoke data contracting and commercialisation projects. Ken has a long track record as a regular contributor to industry dialogue concerning issues at the intersection of technology, business and policy.

Clayton Utz

Level 15
1 Bligh Street
Sydney
NSW 2000
Australia

Tel: +612 9353 4000
Fax: +612 8220 6700
Email: gwilliams@claytonutz.com
Web: www.claytonutz.com

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

There are many solutions to long-standing problems in the healthcare industry that can be addressed with innovative technologies, including those of healthcare providers, patients and regulators.

From a healthcare provider's perspective, advances in digital healthcare may assist in responding to changes in its operating environment (eg, the restrictions created by the COVID-19 pandemic), as well as improved efficiencies and practice management. This includes the adoption of online booking systems for medical practices, telehealth capabilities, and data record-keeping systems.

From a technical perspective, there has been an increase in the prevalence of "do-it-yourself" devices that work with mobile phone apps to allow people to easily monitor their own signs, such as blood oxygenation or electrocardiography. These give practitioners easier access to more comprehensive patient data. At the far end of the spectrum, practitioners may also have increasingly advanced digital medicine options available to deploy, prescribe or administer, such as medical devices that are controlled by software, for example, insulin pumps controlled by mobile phone applications. These technologies are enabled by advances in mobile computing power and internet infrastructure.

From a regulatory perspective, much will turn on the extent to which such products are therapeutic goods regulated under the Therapeutic Goods Act 1989 (Cth) (the "TG Act"). Medical devices are regulated under Chapter 4 of the TG Act, which is administered by the Therapeutic Goods Administration (TGA). The regulation of medical devices is discussed further in **6. Software as a Medical Device**.

1.2 Regulatory Definition

The terms "digital health" and "digital medicine" are not defined in any Australian regulatory framework. There are, however, active organisations in this space that provide definitions for each of these terms.

Digital Health

The term "digital health" is defined by the Australian Government Institute of Health and Welfare as: "An umbrella term referring to a range of technologies that can be used to treat patients and collect and share a person's health information, including mobile health and applications, electronic health records, telehealth and telemedicine, wearable devices, robotics and artificial intelligence."

An example of digital health in Australia is the My Health Record initiative, which is a federal government-operated database that stores an individual's health information in one place. This is regulated by the Australian Digital Health Agency (ADHA).

Digital Medicine

It is more difficult to find a government agency which defines "digital medicine". However, ANDHealth, an organisation established to support the commercialisation of digital medicine in Australia, defines digital medicine as: "Evidence based software and/or hardware products that measure and/or intervene in human health. They all require clinical evidence and are likely to require regulatory approval."

Digital medicine which meets the definition of a medical device will be subject to regulation

by the TGA. On the other hand, many products, including healthcare-enabling technologies, are now excluded from the regulatory regime.

1.3 New Technologies

The key technologies enabling new capabilities in digital healthcare and digital medicine include telemedicine, blockchain electronic health records (or comparable systems such as My Health Record, which uses a public key infrastructure) and artificial intelligence-enabled medical devices.

Digital Healthcare

Since the beginning of the COVID-19 pandemic in early 2020, digital healthcare and its enabling technologies have increased in popularity as the healthcare industry came to rely on technologies to enable consultations with medical practitioners to take place remotely.

This shift, based on necessity, has provided opportunities to improve accessibility and appeal to healthcare for patients who might have had obstacles in attending a consultation previously, including those who live remotely, those who have work or carer commitments, and those with compromised immunity who prefer not to attend a clinic.

At the same time, the federal government's My Health Record has created the potential for medical records to be accessed across medical practices, meaning patients who have not opted out of the programme can be treated by any doctor without needing to have their files transferred manually. If implemented effectively, this has the potential to improve the standard of healthcare provided, as the medical practitioner has all previous tests, results and medical history available to them on the database. However, the use of electronic health records in Australia is in its infancy. Use of the My Health Record system is not yet widespread enough to deliver on its potential benefits. Take-up has been limited by concerns about data security.

Digital Medicine

The most critical development in digital medicine is the increasing prevalence of software which, whether operating alone or in conjunction with certain hardware, operates as a medical device – eg, technologies that can diagnose or at least identify the possible presence of health conditions based upon the application of an algorithm to personal health data which is provided directly by the patient.

Such technologies are instances of "software as a medical device" and will be regulated by the TGA as a standalone medical devices.

1.4 Emerging Legal Issues

Important emerging legal issues in digital health include cybersecurity/data privacy and the boundaries of medical device regulation. The increased use of digital healthcare and rapid innovations in digital medicine have meant that the law has lagged behind in implementing legislation to address the newly created risks associated with these technologies.

Cybersecurity

Cybersecurity concerns are a key emerging legal issue arising from digital health. The increased availability of digital healthcare means that personal health information will increasingly be stored electronically in connected systems, making such information vulnerable to theft. Concerns about cybersecurity have been heightened by a number of high profile data breaches in 2022, including a data breach of Medibank (Australia's largest private health insurer).

Cybersecurity breaches of medical devices that use network functions could result in not only a loss of personal health data privacy, but also changes in device functionality, placing lives at risk.

Healthcare providers using Australia's My Health Record electronic medical records are required by the My Health Records Rule 2016 (Cth) to have a written policy addressing their security arrangements in respect of access to the system, known as a "My Health Record system security policy".

The TGA requires that, where relevant, medical devices should be appropriately cybersecure in order to comply with safety and performance standards under the Therapeutic Goods (Medical Device) Regulations 2002 (the "Medical Device Regulations").

More generally, where personal information is accessed or disclosed without authority and there is a risk that the breach will cause serious harm, the Privacy Act 1988 (Cth) (the "Privacy Act") requires organisations to inform affected individuals and the Office of the Australian Information Commissioner (OAIC) that serious harm may occur.

Medical Device Regulation

The regulation of software-based medical devices by the TGA is another emerging issue, given that digital forms of healthcare have necessarily entailed the proliferation of such devices. It is important to strike the right balance between appropriate regulation of the technology and not limiting the development of new technologies that may not fit neatly into existing categories.

As of 25 February 2021, changes were made to the Medical Device Regulations, clarifying existing requirements, introducing new requirements for software-based medical devices, and expressly exempting or excluding certain types of software from the requirement for registration.

1.5 Impact of COVID-19

COVID-19 has accelerated the uptake of digital healthcare technologies which facilitate the remote delivery of health services.

The benefits of telehealth, as discussed in **1.3 New Technologies**, were crucial during the pandemic. Australia's Medicare system subsidises doctors' provision of most medical services to Australian citizens and permanent residents. Subsidised services are listed on the Medicare Benefits Schedule (MBS). During 2020, the federal government both increased the number of subsidised telehealth services and removed many of the pre-conditions for the provision of existing listed telehealth services.

Those changes were temporary and were originally scheduled to operate until 31 March 2021. They were ultimately extended until 30 June 2022. From 1 July 2022, revised telehealth arrangements continued for some, but not all, subsidised telehealth services. Further adjustments were made to the subsidisation of telehealth services on 1 October 2022 and 1 April 2023.

Similarly, Australia's Pharmaceutical Benefits Scheme (PBS) subsidises the dispensing of prescription medicines. Some high-cost medicines require medical testing before a prescription is authorised. Many of these requirements were temporarily suspended from 1 May 2020. However, the COVID-19 arrangements have now ceased.

The federal government also introduced changes to permit the dispensing of most PBS medicines on the basis of a digital image of a prescription. These measures ceased at the end of March 2023. However, COVID-19 has driven a move to the use of electronic prescribing using secure digital token. Such prescribing is now permitted in most Australian jurisdictions.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

The key regulatory agencies in Australia that oversee technologies, devices and treatment include the following.

Therapeutic Goods Administration (TGA)

The TGA is the medicine and therapeutic regulatory agency of the Australian government, governed by the TG Act. It is responsible for regulating the supply, import, export, manufacturing and advertising of therapeutic goods and it carries out a range of assessment and monitoring activities to ensure that therapeutic goods available in Australia are of an acceptable standard.

Generally, any product for which therapeutic claims are made must, unless there is an applicable exemption, be approved by the TGA for entry on the Australian Register of Therapeutic Goods (ARTG) before it can be legally supplied in Australia.

Australian Digital Health Agency (ADHA)

The ADHA is a statutory authority in charge of implementing Australia's National Digital Health Strategy, which seeks to improve the quality and delivery of healthcare and the Australian health system by digital means.

This organisation manages the Australian My Health Record electronic health record programme. The agency also promotes other forms of digital healthcare, including telehealth and electronic prescription systems, and has an advisory role to the Government Minister for Health regarding the implementation and delivery of national digital health initiatives.an

Australian Health Practitioner Regulation Agency (AHPRA)

AHPRA is the regulatory agency of the Australian government for health practitioners. It is governed by the Health Practitioner Regulation National Laws that operate across the states and territories. The scope of its work includes managing registrations for qualified health practitioners, managing complaints and conducting audits to ensure compliance with national board requirements. AHPRA publishes guidelines for health practitioners in relation to telehealth.

2.2 Recent Regulatory Developments

Regulation of Software-Based Medical Devices

There has been a steady increase in the number of digital medical products available on the market – eg, symptom checkers and diagnostic apps, diabetes management software, and melanoma and skin analysis software. These devices may not fit easily into established pathways for review of the safety and efficacy of health technology. Furthermore, some have been created by developers with limited experience in relation to the requirements for establishing the safety and efficacy of medical devices.

On 25 February 2021, changes were made to the TG Act and the Medical Device Regulations to introduce new classification rules and better define the boundary between software which is regulated as a medical device and software

which is not. The new regulatory regime is discussed further in **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies**.

At the same time, the TGA has introduced changes to the regulation of custom-made medical devices. Custom-made medical devices are and will continue to be exempt from the requirement for registration on the ARTG. However, the changes not only introduce new reporting requirements for manufacturers of custom-made medical devices, but also introduce new categories of medical devices: patient-matched medical devices and medical devices manufactured using a medical device production system (MDPS).

Patient-matched medical devices and MDPSs will need to be included on the ARTG. This is a significant regulatory development to accommodate devices, the production of which is enabled by digital technology (eg, devices which are 3D-printed from a pre-specified design envelope with adaptations to meet the needs of individual patients).

Regulation of Digital Healthcare

In recent years, especially in light of the COVID-19 pandemic, health practitioners have increasingly turned to digital forms of healthcare delivery to overcome barriers to individual access. This not only includes telehealth forms of healthcare delivery that use technology as an alternative to face-to-face consultations, but also digital information systems such as My Health Record, a federal government programme initiated in 2015, which provides an online summary of key health information, electronic prescribing systems, and systems for the home delivery of medication.

The ADHA promotes the use of these technologies and provides regulatory oversight, supporting healthcare integration and delivering improvements to the quality and efficiency of healthcare. For example, the ADHA not only promoted an increase in the use of the My Health Record system, but also expanded the system to include more Australian Immunisations Register information, assisting with the COVID-19 vaccine roll-out. In also engaging in significant education and promotion campaigns, the ADHA allows for greater individual awareness of new forms of healthcare, providing support to these individuals at a time when more traditional forms of healthcare service delivery have been unavailable or inaccessible.

2.3 Regulatory Enforcement

The TGA

The TGA has not identified any specific areas for regulatory enforcement that relate to digital healthcare or digital medicine. More generally, the TGA has a risk-based compliance framework, meaning that its response to low-risk breaches of its regulatory framework will be to educate the infringing party (particularly if that party is not a repeat offender). Its regulatory options escalate to warning letters suspending or cancelling products on the ARTG, right through to enforceable undertakings, the exercise of compulsory powers and ultimately court action.

The changes to the regulatory regimes for software as a medical device and the patient-matched medical devices outlined in **2.2 Recent Regulatory Developments** will result in changed requirements for ARTG listing of existing products. There is a transitional period for sponsors of those products to update their ARTG registrations which runs through to November 2024. It is reasonable to expect that the TGA will be

focused over coming years on ensuring that sponsors update their registrations before the expiry of the transition period.

The ADHA

The ADHA focuses on providing transparent digital health standards, as well as ensuring sustainable governance of these standards. It provides annual reports on the performance of digital health systems, in order to ensure accountability within the sector.

Given the amount of private information that exists within digital healthcare databases, privacy is a key concern of the ADHA. The agency works closely with the Office of the Australian Information Commissioner (OAIC) to maintain privacy and safety across the healthcare system. A Memorandum of Understanding between the ADHA and the OAIC exists to manage the way in which the OAIC provides advice, assistance and independent regulatory services using the personal data in the My Health Record system.

AHPRA

AHPRA provides recourse where serious concerns regarding safe and professional healthcare practices by a practitioner exist. Where a concern is received by AHPRA, it performs a risk assessment of the practitioner in the context of the concern raised.

After assessing concerns, AHPRA may take regulatory action by issuing cautions, imposing conditions on practitioners with a focus on improvement, refer the matter or aspects of the matter for further investigation by, for example, a tribunal or the police, or refer the health practitioner for a health or performance assessment.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

The Australian Competition and Consumer Commission (ACCC)

The ACCC is Australia's competition and consumer protection regulator. It has an important role to play in policing online conduct directed at consumers, including conduct by providers of online health services. Its role includes:

- ensuring that software-based health products are not in breach of competition and consumer laws;
- protecting consumers from misleading and deceptive conduct in relation to online health services; and
- undertaking enforcement action in relation to the misuse of consumer data.

The ACCC has a specialist Digital Platforms Branch and in 2019 published the final report of its Digital Platforms Inquiry. The ACCC is currently conducting a further inquiry in relation to digital platform services (eg, search engines, messaging services and online marketplaces).

In 2018, the ACCC commenced regulatory proceedings against HealthEngine, the operator of Australia's largest online heath marketplace for alleged misleading conduct in relation to its failure to disclose to users of the platform that it was sharing user information with insurance brokers, and its failure to publish negative reviews. In August 2020, the Federal Court ordered that HealthEngine pay AUD2.9 million in penalties in respect of this conduct.

The Office of the Australian Information Commissioner (OAIC)

The OAIC, discussed in **2.3 Regulatory Enforcement**, is the national regulator for privacy and freedom of information. With respect to healthcare, the OAIC has a range of responsibilities regarding data management:

- It handles complaints associated with the collection, use and disclosure of personal health information. This includes a process whereby a person may make a complaint on behalf of a class of persons affected by a breach of the Privacy Act. The OAIC has the power to order the payment of compensation to affected individuals.
- It conducts privacy assessments to ensure that personal information, such as health information, is handled in accordance with legislative requirements. and
- It reports on and conducts investigations in relation to data breaches where personal information, such as health information, is accessed or disclosed without authorisation, or lost.

The Privacy Act recognises information about an individual's health as "sensitive information", meaning that it is subject to additional protections above and beyond those which apply to personal information generally.

The OAIC also has a statutory role under the Privacy Act in approving guidelines for the use of personal information in medical research, which are discussed in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**.

While there are no specific examples of OAIC enforcement action involving the health industry, it has had a role to play in education in relation to the privacy issues arising from the government's My Health Record programme as well as its COVIDsafe App (in respect of both of which the OAIC has been given additional enforcement powers).

While neither agency has enforcement policies at present which specifically target healthcare, both have a particular focus on digital services. As the HealthEngine enforcement action shows, health service providers can be affected by that focus.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

The treatment of preventative and diagnostic care under the Australian health system depends not so much on its classification as preventative or diagnostic, but rather on the nature of the intervention involved.

If an intervention involves the use of a medicine or an in vitro diagnostic device, that intervention will first need to be entered on the ARTG. This involves assessment of the technology in question by the TGA in accordance with the TG Act to ensure that it is of acceptable safety, quality and efficacy. There are different requirements for medicines and medical devices, but the same agency applies those standards.

The reimbursement of such interventions again depends on the nature of the technology involved. Medicines are reimbursed through the PBS. However, more often both preventative and diagnostic interventions involve a medical procedure, which may be reimbursed through Medicare, a government scheme which subsidises the cost of medical procedures.

In order for a preventative or diagnostic procedure to be listed on the Medicare Benefits Schedule, it must be reviewed by the Medical Services Advisory Committee (MSAC). MSAC is an independent scientific committee, established by the Minister for Health to evaluate medical services, health technologies and health programmes proposed for public funding, in order to advise the Minister for Health on whether a medical service, health technology or programme should be publicly funded, and the circumstances in which it should be funded.

Further, many preventative healthcare campaigns involve not only the funding of specific interventions, but also raising public awareness about the availability and importance of such interventions. There is no specific system for the funding public health campaigns. They are funded and run by the government through either the Commonwealth or State Ministers for Health (or both). Current examples of these campaigns include the bowel screening campaign for prevention and early detection of bowel cancer, the breast cancer screening campaign, skin cancer screening campaign and the newly proposed national neonatal screening programme.

The statutory regimes that apply to diagnostic and preventative healthcare include the Competition and Consumer Act 2010 which will apply to any conduct which is in "trade or commerce".

4.2 Increased Preventative Healthcare

There are multiple factors that have contributed to the rise in preventative healthcare. From an Australian perspective this includes population health studies – eg, the 2017–18 National Health Survey – that inform policy, planning and government funding.

These studies have found that the cost and healthcare burdens on Australia's healthcare system could be alleviated by prevention and early detection programmes. Australia's ageing population has informed the preventative healthcare national bowel cancer screening programme, which is free for people aged 50 and over.

Lifestyle factors and social trends also influence preventative healthcare campaigns. An example of this is the beach culture in Australia and the preventative healthcare campaigns around wearing sunscreen and also diagnostic skin cancer checks.

The emergence of COVID-19 highlighted how important it is to have an agile health system focused on prevention and in December 2021 the Australian government introduced a national preventative health strategy for the period 2021–30. The most recent National Budget included AUD6.3 million over three years from 2023-24 to continue the Australian Burden of Disease Study and initiatives to monitor and improve the evidence base of health and wellbeing outcomes, in line with the aforementioned national preventative health strategy 2021–30.

Universally, the advancement in medical technology has improved early disease detection techniques, and the funding of preventative healthcare campaigns has changed the way people view their healthcare providers and encouraged them to become more proactive.

The reason for the change is that it is recognised by governments and insurers that preventative medicine is more cost effective than disease treatment. Whilst there is a wide range of diagnostic testing that is accessible to the public through government funding and private health-

care insurance, there is still a long way to go in further utilising all of the technological advancements in medicine to encourage prevention. There are still highly effective screening tests that are relatively inaccessible to the general public due to their high cost and the absence of a specific reimbursement pathway, for example gene sequencing, which could further assist in the detection and prevention of diseases.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

To the extent that wellness and fitness data comprises personal information, it is likely to be regulated by the Privacy Act 1988 (Cth) (the "Privacy Act").

The Privacy Act takes a relatively expansive view as to what constitutes health information. Health information includes information or an opinion about the health (including an illness, disability, or injury) of an individual, an individual's expressed wishes about the future provision of health services to the individual, and a health service provided or to be provided to an individual. Health information also includes other personal information collected to provide, or in providing, a health service to an individual.

A similarly broad approach is taken to what comprises a health service, and includes activities intended or claimed by the individual or person performing it to assess, maintain or improve the individual's health, as well as those that record the individual's health for the purposes of assessing, maintaining, improving, or managing the individual's health. Health information is a type of sensitive information under the Privacy Act, and consequently more stringent obligations and requirements apply.

The Privacy Act applies to most private healthcare providers, while state and territory legislation applies to public healthcare providers. In some instances, the state and territory legislation (eg, the Health Records and Information Privacy Act 2002 (NSW)) also extends to private healthcare providers.

The Therapeutic Goods Act 1989 (Cth) and the Therapeutic Goods (Medical Devices) Regulations 2002 set out the "Essential Principles" which provide safety requirements for manufacturers regarding the design and production of medical devices. The Essential Principles have been recently amended, including in relation to the management of data and information.

The fitness sector in Australia otherwise remains largely self-regulated, including by the voluntary application by members of Fitness Australia's National Fitness Industry Code of Practice (November 2018) (the "Code"). The Code reiterates each member's privacy law obligations and specifies that each member must not use or disclose to another person confidential information about a consumer obtained under the consumer agreement or by providing fitness services to the consumer unless the information is otherwise lawfully used or disclosed.

4.4 Regulatory Developments

Australian Digital Health Agency (ADHA)

The ADHA is a statutory authority in charge of implementing Australia's National Digital Health Strategy, which seeks to improve the quality and delivery of healthcare and the Australian health system by digital means.

The agency promotes innovative forms of digital healthcare to further proactive and accessible ways to engage with healthcare providers, including telehealth and electronic prescription

systems. The ADHA has an advisory role to the Minister for Health regarding the implementation and delivery of national digital health initiatives and preventative healthcare campaigns.

Medical Services Committee (MSAC)

MSAC is an independent non-statutory committee established by the Minister for Health in 1998. MSAC's main function is to advise the Australian Minister for Health on evidence relating to the safety, effectiveness and cost-effectiveness of new medical technologies and procedures. This advice informs Australian government decisions about public funding for new, and in some cases existing, medical procedures.

The Australian Competition and Consumer Commission (ACCC)

The ACCC is Australia's competition and consumer protection regulator. It is a non-healthcare regulatory authority that applies to preventative healthcare. The Commission oversees the conduct of medical healthcare providers and ensures that common law and practice obligations are adhered to and that anti-competitive conduct, such as market sharing or price fixing, are not adopted as part of a preventative healthcare campaign.

The ACCC has an important role to play in policing conduct directed at consumers, including those arising from preventative healthcare campaigns. Its role includes:

- ensuring that health campaigns and devices are not in breach of competition and consumer laws;
- protecting consumers from misleading and deceptive conduct in relation to health services, advertising and fees; and
- undertaking enforcement action in relation to the misconduct of healthcare providers.

The increase in government-funded, preventative healthcare campaigns and subsidies provided to medical clinics and practitioners who participate in them has meant that the ACCC has needed to focus on the healthcare industry to ensure that doctors or suppliers do not act in an anti-competitive way to obtain the exclusive benefit of such campaigns.

The Office of the Australian Information Commissioner (OAIC)

The OAIC is the national regulator for privacy and freedom of information. With respect to healthcare, the OAIC has a range of responsibilities regarding data management, such as:

- handling complaints associated with the collection, use and disclosure of personal health information (including the power to make compensation orders);
- conducting privacy assessments to ensure that personal information, such as health information, is handled in accordance with legislative requirements; and
- reporting on data breaches where personal information, such as health information, is accessed or disclosed without authorisation, or lost.

The Privacy Act recognises information about an individual's health as "sensitive information", meaning that it is subject to additional protections above and beyond those which apply to personal information generally.

The OAIC also has a statutory role under the Privacy Act in approving guidelines for the use of personal information in medical research, which often informs or forms part of certain preventative medical campaigns.

4.5 Challenges Created by the Role of Non-healthcare Companies

COVID-19 has accelerated the entrance of non-healthcare companies into the market. The companies and their services are diverse, including the entry of certain telecommunications providers and their provision of data-oriented services, e-commerce providers and their provision of entertainment and other services, and certain prominent software companies offering virtual reality technologies.

Non-healthcare companies who develop digital healthcare products find themselves confronting a more thorough regulatory regime than that which may apply to their consumer products. This may mean that the companies lack the necessary specialist skills to navigate that regime. It may also mean that the companies' supply chains are not well adapted to meeting the challenges of health product manufacture. By way of example, a company that moves from the production of consumer electronic products to medical devices may find that its existing suppliers are not able to meet the requirements of Good Manufacturing Practice necessary for the device to satisfy Australian regulatory requirements.

Furthermore, because the provision of health services is highly subsidised in Australia, non-healthcare companies need to identify and navigate the appropriate reimbursement pathways, a process which can take multiple years for some products.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

Connected devices relating to healthcare have become one of the fastest growing categories of the internet of medical things (IoMT) revolution. Many technological developments have contributed to the advent of the IoMT; however, three of the most distinct enablers of the internet of things (IoT) in the medical sector have been improvements in connectivity, advancements in device-embeddable technologies, and greater sophistication in the applications which connect to, control and receive data from those devices. In relation to each of these the following factors are notable:

- improvements in the quality and affordability of connectivity have become central to the IoT, enabling connections across networks between remote devices and front-end applications;
- miniaturisation of sensors has vastly expanded the range of devices which can be connected and enabled; and
- innovations in applications' functionality are rapidly expanding the range of commercially useful IoMT developments that can be pursued.

To date, the most prevalent commercial adoption of IoMT is in monitoring applications and data collection. Sensors embedded in devices can be used to collect and transmit information in relation to heart rate, blood pressure, glucose levels and even information from which a patient's mental state can be determined. Other innovative applications in the development stages include ingestible sensors which can collect

information in relation to stomach pH levels and digestive health, smart asthma inhalers and even smart contact lenses. Remarkably, in addition to monitoring functionality to bolster diagnostic capabilities, IoMT applications are also being conceived and developed for robotic surgery applications, making complex interventional decisions in real time during procedures.

In relation to healthcare developments regarding remote health and in-home care after discharge from hospitals, technologies and regulatory changes enabling telehealth consultations, videoconferencing and remote monitoring through at-home devices has meant that patients can be consulted by medical professionals remotely.

5.2 Legal Implications

The Australian Consumer Law

The principal law governing product safety in Australia is the Australian Consumer Law, which codifies a single set of consumer protection laws for the whole of Australia, including but not limited to laws relating to product safety and product liability.

The Australian Consumer Law is Schedule 2 to the federal Competition and Consumer Act 2010 (Cth). However, its operation across Australia also depends on state and territory laws, which provide that it has effect as a law of each Australian state and territory.

In addition to statutory obligations, product manufacturers and suppliers are subject to obligations under the common law. In particular, persons who are injured by a product may have a right to sue the supplier of the product in negligence (as well as under statutory causes of action created by the Australian Consumer Law). An analysis of a supplier's duty to users of their product in negligence will often be important in assessing the appropriate response to a potential product safety risk.

The Australian Competition and Consumer Commission (ACCC)

The principal Australian product safety regulator is the Australian Competition and Consumer Commission (ACCC), which is responsible for administering the Competition and Consumer Act 2010 (Cth), including the Australian Consumer Law.

The ACCC has regulatory, investigatory and prosecutorial powers granted to it under the Act. In relation to product safety, those powers include the power to require the production of documents or the provision of information, including the power to examine witnesses and to enter premises, conduct searches and seize consumer goods, equipment and documents.

The ACCC also has powers to take a range of actions to protect consumer safety, including commencing compulsory recall actions and issuing product safety notices. Finally, the ACCC can issue penalty notices for breach of Australian Consumer Law or commence proceedings seeking declaratory and injunctive relief as well as civil penalties. It may also refer certain breaches of the Australian Consumer Law to the Commonwealth Director of Public Prosecution for consideration of criminal prosecution, with associated criminal penalties.

Subject to certain carve-outs, the regimes are not exclusive, so that a product that falls, for example, within the TGA's remit, may also be, in some circumstances, a consumer product that is regulated by the ACCC and subject to Australian Consumer Law.

5.3 Cybersecurity and Data Protection

The ever-increasing connectivity between medical devices, applications, healthcare IT systems and other technologies and networks unsurprisingly produces additional cybersecurity risks. These range from device malfunction and loss of data to hacking, information theft and even manipulation of the relevant device. A weakness in any aspect of these connected technologies could result in considerable harm, whether to an individual or more broadly through crippling the vital healthcare infrastructure. New technology also lends itself to new targets, and cybersecurity approaches need to be sufficiently dynamic to combat these emergent threats. Conversely, many healthcare providers also rely on legacy technology without adequate vendor support and updates, exposing those organisations to additional vulnerabilities. This creates a challenging cybersecurity scenario.

The foregoing necessitates a keen focus on, and investment in, cyber-attack prevention and response measures. From a contractual perspective this is being addressed through the introduction of specific cybersecurity and related (eg, privacy, confidentiality) obligations on suppliers, their subcontractors and, where commercially feasible, their full supply chains. This often involves layering certification (eg, compliance with ISO 27001, NIST CSF), regulatory and compliance (eg, privacy requirements including in relation to the notifiable breach scheme, data location and disclosure), penetration and other testing, and cybersecurity insurance requirements, alongside provisions which clearly set out the supplier's day-to-day and other obligations (eg, data encryption, personnel background checks, third party audits).

Accompanying this is the preference of service recipients to impose indemnities for breaching cybersecurity and related obligations (eg, privacy, confidentiality) and to ensure that the supplier's liability in respect of such obligations is sufficient (eg, unlimited or subject to a sizable cap).

Healthcare providers using Australia's My Health Record electronic medical record system are required by the My Health Records Rule 2016 (Cth) to have a written policy addressing their security arrangements in respect of access to the system, known as a 'My Health Record system security policy".

With regard to medical devices, the TGA requires that, where relevant, medical devices should be appropriately cybersecure in order to comply with safety and performance standards under the Therapeutic Goods (Medical Device) Regulations 2002. More generally, where personal information is accessed or disclosed without authority and there is a risk that the breach will cause serious harm, the Privacy Act requires organisations to inform affected individuals and the Office of the Australian Information Commissioner that serious harm may occur.

In December 2022 the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Act 2021 (Cth) came into effect. It has amended the Privacy Act to introduce a binding online privacy code for social media and certain other online platforms as well as increasing penalties for breach of the Act and enhancing enforcement measures.

5.4 Proposed Regulatory Developments

On 31 July 2021, the Australian government opened consultation on options for regulatory reforms and voluntary incentives to strengthen the cybersecurity of Australia's digital economy. The discussion paper, Strengthening Austral-

ia's Cybersecurity Regulations and Incentives, sought views on how the Australian government could incentivise businesses to invest in cybersecurity, including through possible regulatory changes.

Submissions to the discussion paper closed on 27 August 2021. Submissions were made by a diverse range of interested parties including technology providers (eg, Amazon Web Services, Atlassian, Facebook and Telstra), regulators (eg, the OAIC, ACCC and Australian Energy Regulator), industry bodies (eg, the Australian Banking Association and Medical Software Industry Association), and other interested parties (eg, universities). This work formed part of Australia's Cyber Security Strategy 2020 and responded to recommendations of the 2020 Cyber Security Strategy Industry Panel.

On 8 December 2022, and following the above, the Minister for Cyber Security announced the development of the 2023–2030 Australian Cyber Security Strategy. The strategy is designed to help achieve the Australian government's vision of making Australia the most cybersecure nation in the world by 2030. The government is developing cybersecurity policy and initiatives under four key areas:

- a secure economy and thriving cyber ecosystem;
- a secure and resilient critical infrastructure and government sector;
- a sovereign and assured capability to counter cyber threats; and
- Australia as a trusted and influential global cyber leader, working in partnership with its neighbours to lift cybersecurity and build a cyber-resilient region.

The consultation regarding cybersecurity coincided with the Australian government's review of the Privacy Act. On 12 December 2019, the Attorney-General announced that the Australian government would conduct a review of the Privacy Act to ensure privacy settings empower consumers, protect their data and best serve the Australian economy. The review was announced as part of the government's response to the ACCC's Digital Platforms Inquiry. The review has involved obtaining submissions from stakeholders in response to two consultation papers, considering feedback obtained through discussions with stakeholders on specific issues, and through existing research and reports on privacy issues.

In February 2023 the Attorney-General released the final report of the review. The report makes 116 recommendations for amendments to the Act to bring it into line with global standards for data protection. The Attorney-General invited submissions on the report, which were due by 31 March 2023.

There has been a steady increase in the number of digital medical products available on the market – eg, wearable, implantable and digestible healthcare products. These products do not always fit easily into the existing regulatory pathways for review of the safety and efficacy of healthcare.

Amendments have been made to the TG Act and Medical Device Regulations to establish classification systems specific to these new classes of medical device and to exclude some devices (eg, wearable products whose primary focus is fitness) from the registration regime altogether. These amendments are described in more detail in **3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Health-**

care Technologies and 5.1 Internet of Medical Things and Connected Device Environment.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Software will be a medical device (SaMD) if it falls within the definition of a medical device under Section 41BD of the TG Act unless it is the subject of a specific exclusion.

That definition provides that a medical device includes anything (including software) which is intended to be used for:

- human beings for the purposes of diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; and
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or disability,

providing it does not achieve its principal intended action by pharmacological, immunological or metabolic means.

There are different categories of software that could fall within the scope of a regulatory authority, including:

- software as a medical device (SaMD) – software that, on a standalone basis, meets the definition of a medical device;
- software in a medical device (SiMD) – software that is part of a device when it is integral to the functioning of that device and is usually supplied with the hardware device; and
- software that controls a medical device – software that can control or adjust a medical device through a connection, either physical or utilising wireless technology such as Bluetooth or Wi-Fi.

The TGA uses a risk-based approach to regulating medical device technologies by examining the evidence of product risk and comparing it to evidence associated with product benefit. The higher the potential risks of a medical device, the more they need to be examined and monitored.

There are five classifications depending on the level of risk a product poses, class I, IIa, IIb, III and IV.

As described in 2.2 Recent Regulatory Developments, from 25 February 2021, new classification rules were introduced into the Medical Device Regulations for software-based medical devices, providing specific guidance on the classification levels of various types of software-based medical devices, depending on their purpose.

The effect of those changes is, in summary:

- to exclude the following from the category of medical devices:
  - (a) consumer health products which do not provide specific treatment or treatment suggestions;
  - (b) enabling technologies (eg, systems which enable telehealth consultations or the transmission of health information);
  - (c) digitised patient records;
  - (d) population-based data analytics; and
  - (e) laboratory information management systems; and
- to introduce classification rules for:
  - (a) diagnostic or screening software;
  - (b) monitoring software;
  - (c) software which recommends a treatment or intervention; and

(d) software which provides treatment in the form of information,

with the classification rules based, in each case, on the potential consequences of the disease in question and the degree of involvement of a healthcare professional in the process.

The current regulatory regime does not specifically address the use of AI as part of the technology, nor does it deal with the status of software updates. However, a software update is capable of being a recall action in respect of a medical device if it is undertaken for a safety-related reason. Indeed, a 2020 review conducted by the TGA found that in the five years to April 2020, over 20% of medical device recalls were due to software faults.

7. Telehealth

7.1 Role of Telehealth in Healthcare

Please refer to **5.1 Internet of Medical Things and Connected Device Environment** for a discussion of connected devices and the IoMT.

Commercial Adoption of IoMT

To date, the most prevalent commercial adoption of IoMT is in monitoring applications and data collection. Sensors embedded in devices can be used to collect and transmit information in relation to heart rate, blood pressure, glucose levels and even information from which a patient's mental state can be determined. Other innovative applications in the development stages include ingestible sensors which can collect information in relation to stomach pH levels and digestive health, smart asthma inhalers and even smart contact lenses. Remarkably, in addition to monitoring functionality to bolster diagnostic capabilities, IoMT applications are also being conceived and developed for robotic surgery applications, making complex interventional decisions in real time during procedures.

Associated Risks

The opportunities presented by the IoMT naturally come with associated technology and legal risks which, to some degree, correspond to the level of connectivity and functionality exhibited by the relevant solution. These range from device malfunction and loss of data to hacking, information theft and even manipulation of the relevant device. In this regard, modern security protection measures can be adopted to identify network vulnerabilities and moderate the risks of attack.

Legal risks can also arise, especially with respect to traditional legal liability.

- The extent of liability of an IoMT supplier to a healthcare institution, for example, for applications or devices that do not fulfil their stated purposes or that do not operate in the manner intended. This kind of liability may arise from misrepresentation, in negligence, under consumer law (eg, under an implied statutory warranty) or under contract (such as under an express contractual product warranty in the supply contract's terms and conditions). This is further discussed in **15.2 Commercial**.
- The liability to patients of medical or healthcare professionals who rely on the functionality and resilience of IoMT applications or devices, whether for diagnostic or interventional purposes. These issues are discussed in **15.1 Patient Care**.

Regulatory issues may also arise when IoMT applications reach a sufficient level of sophistication to be classified as medical devices. This

is explored further in **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies**.

7.2 Regulatory Environment

Many regulatory changes were made in response to the COVID-19 pandemic, with the focus on facilitating digital healthcare so that practitioners could respond to isolation requirements while continuing to offer consultations and treat patients.

Electronic Prescriptions

The National Health (Pharmaceutical Benefits) Regulations 2017 (Cth) were relaxed to permit electronic prescriptions or "e-prescriptions" under the Pharmaceutical Benefits Scheme (PBS). As explained in **1.5 Impact of COVID-19**, this allowed digital copies of prescriptions to be sent directly to pharmacies. The process still allows the patient to nominate their preferred pharmacy, as long as it has the facilities required to receive the e-prescription. These arrangements ended on 31 March 2023. However, arrangements are now in place in most Australian jurisdictions (although there is not consistency in the form of those arrangements) which permit prescriptions to be delivered by electronic token.

Videoconferencing Platforms

Videoconferencing platforms such as Zoom and Microsoft Teams have not been subjected to any regulation specifically aimed at telehealth. In fact, Allied Health Professionals Australia recommends Zoom and Skype as having useful features for telehealth. It does, however, also recommend the platforms designed specifically for telehealth, Coviu and Cliniko. Nonetheless, all telehealth consultations remain subject to the Privacy Act 1988 (Cth). While the Privacy Act does not specifically govern telehealth, practitioners must remain aware of their statutory obligations under it, as well as any relevant state and territory regimes.

7.3 Payment and Reimbursement

As discussed in **4.1 Preventative Versus Diagnostic Healthcare**, most medical practitioners' services are subsidised by the federal government through Medicare. From 13 March 2020 to 30 June 2022, temporary MBS items were introduced allowing many reimbursed services to be provided by telehealth. The federal government also increased certain incentives for medical practitioners, to encourage an increased uptake of telehealth appointments for suitable issues.

From 1 July 2022 permanent arrangements were put in place which preserved many, although not all, of the telehealth MBS items. Those arrangements were further modified on 1 October 2022 and 1 April 2023, including by the introduction of rules intends to prevent the overservicing through telehealth.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

Please refer to **7.1 Role of Telehealth in Healthcare**.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

The key distinguishing feature of 5G networks as compared to their predecessors, most relevantly 4G networks, is the ability to transfer greater volumes of data at significantly higher

speeds, across lower latency connections. For example, 5G networks can reach speeds of up to 100 times faster than 4G networks and can reduce the delay between sending and receiving data from 200 milliseconds to 1 millisecond.

These advances mean that more data can be transmitted between the healthcare provider and the patient, and also that the provider can see such data in close to real time. At a basic level, provided that the hardware exists to measure a patient's physiology, this opens the possibility to remote consultations moving closer to what is currently possible in a face-to-face consultation, including in terms of a healthcare provider's ability to test the patient's symptoms and diagnose the patient by way of a virtual experience that more closely resembles a traditional physical consultation. Once these technologies exist, it is possible to imagine many applications for them.

For example, it is possible to imagine first responders to medical emergencies being equipped with portable patient monitoring systems. Data from those systems could be relayed to appropriate specialists who could advise about critical treatment needs and assist to triage the patients.

Of course, the more dependent a healthcare service becomes on a particular technology, the more difficult it is to cope with a failure of that technology. If 5G technologies come to be relied upon to facilitate the delivery of critical health services, those who are providing those services will have high expectations of the reliability, reach and security of those services, as well as critical service-level expectations in the event of a service failure. Equally, however, tensions may arise between the service-quality expectations of those administering the services and the risk appetite of upstream suppliers of standard products and services. These are matters which will need to be considered in entering into any contract for the provision of 5G services to support critical health infrastructure.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

The Privacy Act

The collection, storage and use of health information is regulated by the Privacy Act, as well as by health information-specific legislation in some of the Australian states and territories (NSW, Victoria and the ACT). State and territory legislation generally agrees with the Privacy Act, as least with respect to the manner in which consent to the collection and use of personal information is obtained.

The Privacy Act contains some specific provisions which deal with the use of health information for medical research. While it is preferable that the collection of health information for research purposes is the subject of specific consent, Section 16B of the Privacy Act provides for an exemption for private industry from the usual requirements of consent if a "permitted health situation" exists. "Permitted health situations" include situations where:

- the collection, use or disclosure of data is necessary for research or the compilation or analysis of statistics relevant to public health or public safety;
- in the case of collection, the purpose cannot be served by the collection of de-identified information;

- it is impracticable to obtain individuals' consent to the collection, use or disclosure of their data; and
- the collection, use or disclosure of data is undertaken in accordance with the relevant guidelines published under the Privacy Act.

Guidelines

The guidelines in question are the guidelines approved under Section 95A of the Privacy Act published by the National Health and Medical Research Council (NHMRC) and approved by the OAIC. The guidelines provide, among other things, that any proposal to use personal information in medical research must be approved by a Human Research Ethics Committee.

There are also separate guidelines published by the NHMRC and approved by the OAIC pursuant to Section 95 of the Privacy Act which relate to the use of personal information in medical research by public agencies.

De-identified Information

The Privacy Act does not apply to the use of de-identified information. However, the NHMRC also publishes the National Statement on Ethical Conduct in Human Research which deals with the appropriate conduct of medical research in Australia (and is the standard against which Human Research Ethics Committees approve the conduct of such research).

Clause 2.2.7 of the National Statement provides that, "Whether or not participants will be identified, research should be designed so that each participant's voluntary decision to participate will be clearly established." While this provision should not be read as a blanket prohibition on the use of de-identified data for research purposes, it does mean that it is preferable that patients are aware of how their health data will be used.

There are no specific rules or guidelines as to how consent to the collection or use of personal information must be obtained in a digital context. The collection of sensitive information, including health information, is subject to stricter requirements for obtaining consent than is the case for other forms of information. However, there is no need under Australian law for a specific collection statement. Rather, what is required is that in all circumstances it can be shown that the individual has provided unambiguous and specific consent to the collection of their health information for a specific purpose.

The Privacy Act also includes a data breach regime, administered by the OAIC. It requires organisations to report unauthorised access to or disclosure of personal information which may result in serious harm to any of the individuals to whom the information relates. The Privacy Act also permits individuals to complain to the OAIC in respect of interference with their privacy. The OAIC has the power, following investigation of a complaint, to declare that a breach has occurred and that a person or entity must perform certain acts or pay compensation by way of redress.

Finally, as the HealthEngine case discussed in **3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies** makes clear, undisclosed use of personal information may give rise to breaches of general consumer law prohibitions on false, misleading or deceptive conduct.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

AI's Present Role

According to some, AI is demonstrated when a machine becomes capable of emulating and applying true cognitive decision-making, self-learning from its own prior decisions and adaptively adjusting its own future decisions based on historical experience. In the IoMT context, many of the applications and devices initially deployed (such as the remote monitoring and assistive technologies referred to in **8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things**) are, at least for now, better described as assisting and augmenting human decision-making as opposed to completely replacing it. In this respect, the primary role of these types of technologies is to provide a richer basis for the exercise of human judgement.

The Next Era of AI

Equally, however, there is also emerging recognition that significant potential exists for the next era of AI to expeditiously problem-solve, rigorously reason and apply judgement within appropriate decision parameters. Furthermore, significant resources are being furiously applied to developing independent machine learning capability – ie, machines which can improve and define their own decision processes without the need for specific human enhancement. If this can be achieved, then the implications for IoMT are significant. New IoMT applications could lead to continuously improving diagnostic capabilities, reduction in error rates, improved procedural success rates and better patient outcomes. Another key hope for digital healthcare is that IoMT will come to provide robotic assistance to interventional clinicians during medical procedures and even generate model data sets for training purposes.

The processing and interpretation of data is closely linked to the future of AI in modern healthcare. A significant advantage of computer-assisted technology over human clinicians is the capacity to analyse, process and determine patterns in vast data sets with a speed and consistency of approach that would not otherwise be possible. This would enable a new era of deductive or predictive medicine, in which systems can review data and identify patterns and characteristics which would be unrecognisable by a clinician. For instance, in Mount Sinai Hospital, New York in 2016, a computer program was trained using the electronic health records of 700,000 patients and then used to predict disease in a select sample of 76,214 patients in the "Deep Patient" initiative. Researchers noted that the results significantly outperformed those obtained from alternative learning strategies applied to original raw health records.

Risks Associated With AI in IoMT

Commentators have highlighted various risks associated with the overly rapid adoption and implementation of AI-based technologies, including the influence of machine and algorithmic bias, a failure to appreciate non-quantitative nuance and the possibility that future over-reliance on technologies may lead to a lower level of skills in future generations of medical professionals. These risks will need to be cautiously approached and managed as technologies are tested and deployed.

11.2 AI and Machine Learning Data Under Privacy Regulations

Addressing Potential Bias in AI and Machine Learning

Despite its benefits, the use of AI comes with several unique risks and challenges. The use of AI raises a number of ethical considerations, especially where AI is deployed to make decisions which can potentially adversely impact the rights and interests of individuals. Although AI can reduce the element of human cognitive biases, it has the potential to introduce algorithmic biases and to operate unfairly based on flawed algorithms. For example, there was a flawed algorithm in the Commonwealth's "RoboDebt" scheme where the process used by the AI algorithm made certain incorrect assumptions resulting in some requests for the payment of money which was not in fact owed.

The potential for bias in AI and machine learning is being increasingly considered by Australian state and territory governments, human rights bodies, and other commentators. In June 2023 the Australian government released its "Safe and responsible AI in Australia" discussion paper which seeks comments regarding the Australian government's regulatory responses to AI. This paper refers to the Royal Australian and New Zealand College of Radiologists (RANZR's) "Ethical Principles for Artificial Intelligence in Medicine" which contains nine ethical principles to "guide the development of professional and practice standards regarding the research and deployment of machine learning systems (ML) and artificial intelligence tools (AI) in medicine".

Further, the New South Wales (NSW) government's AI Policy and Assurance Framework provides guidance on the safe use of AI, finding the balance between opportunity and risk, while putting in place those protections that would apply for any service delivery solution.

There also exist AI Ethics Principles and Policies at both a federal and state and territory level in Australia. Australia's AI Ethics Principles set out eight principles designed to ensure AI is safe, secure and reliable. Further, the NSW government's AI Ethics Policy (August 2020) sets out mandatory ethical principles for the use of AI, including that the use of AI must include safeguards to ensure that potential data biases are identified and appropriately managed and that data models are designed with a focus on diversity and inclusion. The Australian Human Rights Commission's technical paper "Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias technical (24 November 2020)" identifies that algorithmic bias can cause real harm, that there is a legal imperative to address this risk, and that rigorous design, testing and monitoring can avoid algorithmic bias.

The dialogue continues, with Australia's Chief Scientist Dr Cathy Foley last year sharing her thoughts on the importance of ethics and diversity when creating next generation technologies, and that algorithms can use flawed datasets which contain inherent biases because of the inequalities in society.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

In the recent High Court decision of Calidad [2020] HCA 41 (here), the Court affirmed for the first time in Australia the doctrine of exhaustion of patent rights, and in so doing, overturned

more than a century of jurisprudence under the alternative "implied licence" doctrine.

The Court confirmed that once a patentee (or someone with the patentee's authorisation) sells or supplies patent-protected goods, the patent rights in respect of the sale or supply of those goods are exhausted, which means that (as a matter of patent law) there is nothing preventing the customer from improving the product (eg, to extend its useful working life), and then selling/supplying the products commercially without the patentee's authorisation.

Following this landmark decision, patentees (and their licensees) who sell or supply patent-protected goods to third parties should now seek greater contractual protections in respect of what the customer can do or – more importantly – cannot do, with the acquired goods, if the patentee would seek to restrict the customer's ability to improve and re-sell the products.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

The enhanced digital healthcare solutions of the future will require the coalescence of a range of enabling factors, including accessibility to robust and resilient telecommunications connections, modern software solutions, data transfer and storage solutions, and ongoing advancements in nanotechnologies to enable further miniaturisation of "smart devices". In Australia, various steps are being taken to enable these developments.

The Australian government is currently undertaking a landmark national broadband network (NBN) roll-out, which involves the deployment of a multi-technology mix of telecommunications infrastructure across the country. This is a major transformative initiative in the Australian telecommunications industry. Relevantly, significant commentary in relation to the business proposition for the NBN project focused on the potential benefits of improved access to telehealth solutions, particularly for regional Australians, and the richness of new health-related applications that could be supported by high-bandwidth connectivity. At the customer's end, the IT infrastructure of healthcare institutions, medical centres and other organisations will need to evolve to be capable of receiving and benefiting from this improved connectivity.

The Australian healthcare sector is experiencing a steady proliferation of new software and applications which are designed to support or facilitate diagnostic activities. Based on industry commentary, there appear to be mixed views among Australian medical professionals in relation to the utility of machine or software-based diagnostic tools. One view is that advancements in AI and software-based tools represent a vital tool in improving diagnostic reliability, by offering an invaluable initial assessment for further human interrogation or by way of a useful cross-check against human-based primary assessments. The contrary view is that, for seasoned medical professionals, the need to have regard to machine-based assessments and navigate false-positive machine-generated diagnoses simply adds to case review time without necessarily improving substantive diagnostic or patient care outcomes. As machine learning and medical software solutions evolve in functionality and sophistication, it is likely that confidence in AI-based tools will continue to improve, encouraging their adoption.

Data storage solutions are becoming an increasingly essential part of modern healthcare applications, including those applications which rely

on the hosting, management and retrieval of large data sets. The uptake of these kinds of applications has been accelerated by the move to cloud-based solutions and the growing mobility of medical professionals, as distinct from the traditional approach of hospitals, medical centres and other institutions maintaining local storage solutions for their healthcare and patient information.

Focus on Safeguarding and Protecting Healthcare Information

The corollary of greater levels of patient and healthcare information being held in and communicated through third-party data services is a higher level of sensitivity in relation to the safeguarding and protection of that information from unauthorised use and disclosure. To the extent that such services are relied on to maintain the sole repository of an organisation's healthcare information, this also places a greater focus on ensuring that mechanisms exist to enable the recovery or restoration of that data in the event of loss or corruption. For this reason, many contracts in the healthcare space have come to include comprehensive provisions relating to privacy, security, data protection and recovery, which bolster the statutory obligations applying to health information (being a sensitive category of personal information) under the Privacy Act.

13.2 Data Management and Regulatory Impact

We are not aware of any proposed or enacted regulations that specifically concern the implementation of IT upgrades. However, it can be the case that IT upgrades are necessitated by other regulatory developments (eg, the implementation of privacy and data protection requirements). Further, it is clear that software is treated as "goods" under Australian Consumer Law meaning that manufacturers and suppliers of software will be subject to, among other things, consumer guarantees in respect of their software which cannot be excluded by contract.

14. Intellectual Property

14.1 Scope of Protection

Patent Law

Patent law may protect an invention in digital health that meets the standard requirements under the Patents Act 1990 (Cth). An invention must be a manner of manufacture that is new, useful and involves an inventive step. This means business methods will not be patentable unless they involve the direct application of a physical form or device, in a technically innovative way, to bring about a useful result. Mere schemes implemented using generic software will not constitute patentable subject matter (eg, Encompass Corporation Pty Ltd v InfoTrack Pty Ltd (2019) 145 IPR 1).

Copyright Law

Copyright law will protect an original literary work (such as computer code) that is the product of an identifiable human author or authors. This means the original literary work must be the product of independent human intellectual effort directed to the creation of the material form of that work (eg, Telstra Corp Ltd v Phone Directories Co Pty Ltd (2010) 90 IPR 1).

Databases

There is no database right under Australian law per se. Australian law also offers no protection for databases that are created without direct human authorship. Works of authorship created by AI technologies, without any substantive human input, are not protected or owned by anyone, even if the computer code behind an AI was authored by a human and is itself protected.

Secrets

Trade secrets can be protected as confidential information by way of contract or equity. By ensuring anyone with access to trade secrets is bound by appropriate obligations of confidence, such as in the terms of an employment contract or non-disclosure agreement, the confidentiality claimant can enforce any breach of those contractual obligations. If no contractual obligation exists in relation to the trade secret, a confidentiality claimant may be able to bring an equitable action for breach of confidence.

14.2 Advantages and Disadvantages of Protections

Different forms of IP protection will be better suited to different types of innovation/creation. Commercialisation strategy also plays an important part in deciding what form of protection to seek and when to do so. The following comments give a high-level overview of some of the relevant considerations.

Copyright

Where innovation lies in the way in which an idea has actually been expressed, in material form, copyright protection may be a suitable form of protection to prevent third parties from copying that work. An advantage of copyright is that it subsists upon the creation of an original work; there is no requirement to register any copyright claims in Australia. A disadvantage of copyright is that it does not protect the idea itself (as opposed to the expression of the idea), which means it is generally ill suited to protecting new and valuable ideas that can be easily replicated in material form by third parties without copying the original work itself.

Patents

Where value lies in an inventive concept itself, which can be applied industrially in one or more ways, patent protection may be a better suited form of IP. Patents offer a patentee a limited monopoly to exploit the claimed invention (generally 20 years for a standard Australian patent), in exchange for the patentee disclosing to the public at large the nature of the invention and how to perform it. Patents have the advantage of protecting different embodiments of the claimed invention. They are also generally well suited for technology where details of the working of technology will need to be disclosed publicly in order to commercialise the product (as is typically the case with healthcare products, where lots of information is disclosed publicly through the regulatory approval process). A particular disadvantage of patent protection is the cost involved in enforcing patent rights. The limited duration means patents are also generally ill-suited to innovations in respect of which 20 years is insufficient time to realise the commercial value before exclusivity is lost.

Trade Secrets

Trade Secrets (ie, information bound by obligations of confidentiality in contract or equity) are another important form of protection. The primary advantage of trade secrets is that they do not expire. Thus, if confidentiality obligations are enforced rigorously, the information may in theory be protected from third parties indefinitely. Trade secrets are generally ill-suited to products or inventions where the act of commercialising the product will necessarily involve the disclosure of its working to the public (as is typically the case with healthcare products). In those circumstances, patent protection may be more appropriate.

14.3 Licensing Structures

Contractual licensing arrangements for IP rights in digital healthcare can adopt a broad range of different structures. At a high level, licences to

exploit IP rights can be either exclusive, sole, or non-exclusive. For some IP rights, such as patent rights, an "exclusive licence" has a special meaning under the relevant legislation, as meaning a licence where the owner licenses all the rights to another person, to the exclusion of all others - including the actual owner. A properly constituted "exclusive licence" may enable the exclusive licensee to commence infringement proceedings against third parties, without needing the owner's consent (although the owner must generally be joined as a party to such proceedings).

Licensing structures may otherwise be customised to suit the needs and commercial objectives of the parties. They can be perpetual or for a limited term. They may be irrevocable, or revocable upon certain circumstances arising (such as non-payment of royalties). They may be royalty free or have a payment structure involving anything from the simplest per-unit royalty rate to the most complex formula for calculating costs and revenues and allocating them as between the parties to the licence.

14.4 Research in Academic Institutions

Inventions and works of authorship that are the product of joint inventors or authors may not be exploited by third parties without the consent of all of the co-inventors or co-authors. A single co-owner of copyright or a patent cannot authorise a third party to exercise the exclusive rights afforded by that copyright/patent without licence from the other co-owners. In practice, this means co-owned IP rights may be more difficult to commercialise, and therefore of lower commercial value, than such rights owned by a single entity.

14.5 Contracts and Collaborative Developments

Inventions and works of authorship that are the product of joint inventors or authors may not be exploited by third parties without the consent of all of the co-inventors or co-authors. A single co-owner of copyright or a patent cannot authorise a third party to exercise the exclusive rights afforded by that copyright/patent without licence from the other co-owners. In practice, this means co-owned IP rights may be more difficult to commercialise and, therefore, of lower commercial value, than such rights owned by a single entity.

15. Liability

15.1 Patient Care

Functional Approach to Regulation of Technology

Fundamentally, the traditional approach of the Australian legislature has been to avoid technology-prescriptive regulation and instead impose functional requirements in a technology-agnostic way. This has been a consistent theme across a range of sectors. This philosophical approach often stands in contra-distinction to European-based directives or statutory requirements in other countries, which can be more technology-specific in nature (eg, in relation to mandating particular technology standards relating to data transfer, encryption levels and electronic attestation). Generally, Australian laws, which are predicated on, or which relate to a base assumption of human decision-making have not evolved to mandate the adoption of particular technology standards as a substitute for that human decision-making process, nor to automatically alleviate responsibility for a human decision based merely on reliance on a prescribed technology process.

Liability for Decisions Based on AI Solutions

In Australia, liability for medical decisions with an impact on patient outcomes will often be determined according to the common law tort of negligence. Establishing negligence relies on demonstrating the existence of a duty of care, defining the appropriate standard of that duty, proving that such standard has been breached and showing that a certain measure of damages has flowed from the breach. The determination of these various elements will always depend on the specific facts and circumstances of a particular case; however, no general rule or principle exists to the effect that a medical professional who exclusively relied on an AI-based solution in substitution of their own judgement will be exempted from liability. Relevant factors will include the extent to which it was reasonable to rely on a machine-based assessment, the extent to which the medical professional was reliant (eg, whether in relation to the interrogation of specific data points or in relation to an overall AI-based recommendation) and potentially, to some degree, the level of sophistication of the solution provided by the AI and the proven integrity of its outputs.

It is also likely that the developers of such systems could be liable to patients for their consequences both under theories of negligence and under statutory liability regimes which impose liability on manufacturers of goods.

15.2 Commercial

Where a third-party vendor supplies products or services to support the operations of hospitals, medical centres or other healthcare institutions, the liability for the non-performance or non-conformity of those products or services with their intended requirements will typically be regulated by the applicable contract of supply. The terms and conditions of that supply contract will usually, assuming it is consistent with best practice:

- contain various warranties, performance and delivery comments in relation to the applicable products and services;
- outline security (including cybersecurity), data protection, disaster recovery and business continuity obligations owed by the vendor;
- include indemnities in relation to particular kinds of risks that could create exposure for the customer, including in relation to the third-party vendor's breaches of law or regulatory requirements and other types of third-party claims brought against the healthcare institution as a result of the vendor's activities; and
- set out a contractual allocation of risk in relation to legal claims arising in relation to the contract or its subject matter.

The extent of the vendor's liability and how risks are contractually allocated will largely depend on the parties' commercial understanding with respect to the relevant scope of the products and services. For instance, it may not be appropriate for a third-party vendor to indemnify the customer against all cybersecurity attacks if it is only responsible for providing a discrete solution for the customer's deployment and is not otherwise assuming responsibility for the security and integrity of the customer's network environment in which that solution will be deployed and implemented. In such circumstances, the vendor's liability may be more appropriately confined to security vulnerabilities in the solution itself. Conversely, if security management and network integrity fall within the scope of the professional services the vendor is supplying, then a greater level of contractual protection against such events would be justified.

The contract of supply will usually also outline how any limitations on the vendor's liability interact with any common law claims arising from its activities (eg, arising in negligence) and, to the extent that it can be legally altered by the contract, any statutory liability.

BELGIUM

Law and Practice

Contributed by:
Olivier Van Obberghen, Pieter Wyckmans, Amber Cockx and Chaline Sempels
QUINZ

Contents

QUINZ is a Brussels-based law firm with a strong focus on life sciences. Quinz assists the global, regional (Europe, the Middle East and Africa (EMEA), Latin America (LATAM), Asia-Pacific (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 sound expertise in regional and local regulatory work (including pricing and reimbursement, clinical trials, data transparency, marketing authorisation procedures, current good manufacturing practice (CGMP) and compliance matters (including transfers of value, promotion of life sciences products, antitrust compliance questions, patient-directed programmes)), and the General Data Protection Regulation. Quinz was founded in 2011. Its life sciences department is headed by Pieter Wyckmans and Olivier Van Obberghen. Clients include Janssen Pharmaceutica, UCB, Takeda, Novo Nordisk, and Roche.

Authors

Olivier Van Obberghen was trained as an M&A and commercial transactions lawyer. Since 2009, Olivier has worked exclusively for clients in the life sciences and innovative technologies sectors. He co-heads the life sciences department of Quinz. Olivier's expertise in the life sciences sector covers the entire life cycle of a drug product (R&D, clinical trials, supply chain and technical operations, commercial distribution), including M&A, product divestments and licensing deals. Since 2013, Olivier's practice has focused on healthcare compliance, tackling questions on the promotion of drug products and medical devices, on interactions with healthcare professionals/healthcare organisations, on patient-support programmes, and on the use (and commercialisation) of healthcare data. Olivier worked in-house for the legal department of UCB.

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. His transactional expertise covers the entire life cycle of a drug product (R&D, clinical trials, supply chain and technical operations, commercial distribution), including M&A, product divestments and licensing deals. Pieter has developed a particular life sciences regulatory expertise under EU and national laws. More specifically, he provides his clients with expert advice on a broad array of legal and strategic issues regarding clinical trials and market access, including early-access programmes, marketing authorisation procedures, and pricing and reimbursement. Pieter worked in-house for the legal department of UCB.

Amber Cockx is a lawyer with a main focus on the life sciences sector, as she provides transactional and regulatory support to clients active in the pharmaceutical and medical devices industry. Her areas of expertise include transactional and regulatory assistance throughout the entire product life cycle, from negotiating and drafting contracts to all aspects of data protection and privacy laws, clinical trials, marketing authorisations, advertising and promotion, pricing and reimbursement, and interactions with healthcare professionals and healthcare organisations.

Chaline Sempels is a lawyer focusing on the life sciences industry, including digital health. She supports clients ranging from innovative start-up ventures to multinational corporations in (strategic) transactions and European regulatory affairs, throughout the entire product life cycle. In this context, her main areas of expertise include negotiating and drafting (supply chain and distribution) agreements, co-ordination of international R&D collaborations (the Horizon 2020 funding programme, the Innovative Medicines Initiative (IMI2) programme), medical devices, software applications and emerging technologies, and interactions with healthcare professionals and organisations.

QUINZ

Medialaan 28B
1800 Vilvoorde
Belgium

Tel: +322 557 380
Fax: +322 534 219
Email: info@quinz.be
Web: www.quinz.be

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Digital healthcare is an umbrella term that stands for the use of information and communication technologies (ICT) – and, in particular, internet technology – to support or improve healthcare in the broadest sense, including e-health platforms, electronic patient files, electronic drug prescriptions, teleconsultations, and medical, fitness and well-being applications (apps).

Digital medicine and digital therapeutics (DTx) are subsets of digital healthcare and hence conceptually fall within its broad scope. The difference between both concepts, however, might be hard to distinguish. Digital medicine refers to the deployment of technologies as tools for diagnosis and intervention to improve human health (eg, clinical decision support software) whereas DTx refers to evidence-based therapeutic interventions driven by software to prevent, manage or treat a medical disorder or disease and to spur changes in patient behaviour (eg, wearables and other wireless devices). They include patient-facing software apps that therapeutically support patients, bear the CE marking (see **6. Software as a Medical Device**) and have a proven clinical benefit. Typically, DTx is classified as a subcategory of digital medicine.

Regulatory oversight, including the need for clinical evidence, will be critical in the context of digital medicine and DTx products and services due to their deployment for interventional, diagnostic and therapeutic purposes. In addition, these products will often meet the definition of a medical device, hence requiring compliance with applicable medical device legislation.

Both from a healthcare provider and patient/consumer perspective, it can be assumed that digital healthcare technologies, in general, will be – and already are – more rapidly and widely embedded into society due to their supportive and facilitative character. It is very likely, however, that some of these products will be received more sceptically by patients due to their more "invasive" nature (eg, insideables).

1.2 Regulatory Definition

Neither "digital health" nor "digital medicine" or "DTx" is currently defined in the Belgian regulatory framework.

1.3 New Technologies

As the main technologies in digital healthcare are likely to be focused on the collection, processing, transmission and presentation of data, technologies such as cloud computing, communication technologies, wireless networks (such as 5G – see **9.1 The Impact of 5G Networks on Digital Healthcare**) and big data will remain essential. Nevertheless, the importance of other technologies such as robotics, virtual reality and the internet of medical things (IoMT) cannot be underestimated.

Technologies (that can be) deployed in the context of digital medicine and DTx are equally numerous and include:

- personal genomics (which is expected to play an important role in personalised and predictive medicine);
- artificial intelligence (AI) (which may contribute to more accurate diagnosis);
- robot-assisted surgery; and
- wearables and sensors (which can be used for continuous and remote monitoring of vital functions of patients).

1.4 Emerging Legal Issues

Novel health technologies (eg, AI, the IoMT, 5G networks and Bluetooth) are challenging the boundaries of the Belgian regulatory framework, which is often ill adapted to address the legal concerns such technologies entail. Existing laws and regulations scarcely accommodate for the questions raised as a result of a continuously developing digital healthcare industry, including with regard to:

- data protection and privacy (eg, illegitimate processing of personal data);
- cybersecurity (eg, ransomware);
- intellectual property protection (eg, can AI be an inventor?);
- liability (eg, can AI be liable?);
- reimbursement (eg, telehealth); and
- compliance (eg, CE markings).

The digitalisation of healthcare also involves a number of actors entering the industry that are unfamiliar with the highly regulated framework in which health products are embedded, which requires additional compliance investments. As a final point, the emergence of AI-driven healthcare technologies might involve ethical considerations regarding privacy, bias and discrimination in healthcare.

1.5 Impact of COVID-19

The COVID-19 crisis has brought the digitalisation of public health to the forefront, increasing the pace of the application of digital healthcare products (eg, the increased use of medical, fitness and well-being apps). Radical social distancing measures and the need to reduce pressure on hospital units resulted in clusters of emergency telehealth measures being adopted. Many patients accessed their online personal health viewer for the first time to consult their COVID-19 test results. The Belgian Data Protection Authority relentlessly advised on temperature checks, contact tracing and the (lack of) employer prerogatives at the workplace.

While the success of some of these initiatives may have been modest, the shifted attitudes of patients, healthcare providers and regulators towards digital healthcare technologies are likely here to stay.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

The Federal Agency for Medicines and Health Products (FAMHP) is the Belgian national competent authority overseeing the quality, safety and efficacy of medicines and health products, including medical devices, both during the clinical development process and with regard to the authorisation and marketing of drug and health products. To the extent digital health products are considered medical devices, they fall within the scope of the authority of the FAMHP. The actual conformity assessment procedure for granting the CE marking is carried out by the so-called “notified bodies” designated by the FAMHP.

The Federal Public Service for Health is more generally responsible for the organisation of healthcare in Belgium and controls the quality of health services and the practice of healthcare professionals. Hence, the deployment of digital medicine and DTx products and services by healthcare professionals and/or institutions is subject to regulation originating from this governmental agency and healthcare professionals have certain reporting obligations to its organs. In addition, the National Institute for Health and Disability Insurance (NIHDI) establishes reim-

bursement schemes for healthcare services, medicines and health products and thereby exerts an important influence on (the conditions for reimbursement of) health products and treatments. Lastly, professional associations such as the Order of Physicians and the Order of Pharmacists impose deontological obligations on healthcare professions, while self-regulatory industry organisations such as pharma.be and beMedTech lay down ethical rules for pharmaceutical and medical device companies.

2.2 Recent Regulatory Developments

Legislation specific to the area of digital healthcare is still very limited in Belgium. After a long transition period, Regulation (EU) 2017/745 (the Medical Device Regulation, or MDR) is applicable as of 26 May 2021 (although medical device manufacturers may be able to benefit from additional time within which to achieve MDR compliance) and Regulation (EU) 2017/746 (the In Vitro Diagnostic Medical Device Regulation, or IVDR) applies as of 26 May 2022. The Acts of 22 December 2020 and 15 June 2022 have brought the Belgian regulatory framework in line with the new EU legislation.

In January 2021, the NIHDI launched a scheme for the reimbursement of mobile health apps (as further discussed under **4.4 Regulatory Developments**).

Additionally, electronic prescribing has been mandatory as of the beginning of 2020. The Healthcare Quality of Practice Act of 22 September 2019 safeguarding privacy, safety and quality of healthcare came into force on 1 July 2022, and impacts the permissibility of providing certain health services via digital means.

Finally, several legislative proposals in light of the European data strategy (which will undoubtedly have a considerable impact on the digital healthcare industry) have also been adopted in recent months, as further discussed under **3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies**. One of the most notable examples thereof would be the legislative proposal on "The European Health Data Space" launched by the European Commission on 3 May 2022, which aims to create a framework for the sharing of health data across the EU (as discussed under **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**).

2.3 Regulatory Enforcement

Enforcement concerning digital healthcare has been limited in Belgium up until this point. The main areas of enforcement concern data protection infringements, violations of the rules governing the marketing and sale of medical devices and competition considerations.

However, healthcare regulatory authorities have increasingly been on guard since the beginning of the COVID-19 crisis and the medtech industry will likely become an enforcement priority in the next few years due to the application of the MDR and the IVDR.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

The increasing digitalisation of the healthcare industry is causing healthcare professionals and businesses to be impacted incrementally by legislators regulating digital markets. For instance, the European Union recently launched several legislative initiatives governing digital markets,

goods and services (including the Digital Services Act and the Digital Markets Act and the proposed regulations for the Data Act and the Data Governance Act) and a proposal to regulate AI (see **11.2 AI and Machine Learning Data Under Privacy Regulations**).

In addition, both the European Commission and the Belgian Competition Authority have focused their enforcement efforts on the digital market in recent years. Moreover, the healthcare industry is continuously looking for guidance from, and engaging with, data protection authorities such as the Belgian Data Protection Authority and the European Data Protection Board to manage the challenges that accompany the introduction of novel technologies in the sector. Several regulatory agencies also take on a different role with regard to new health products. Where the Federal Public Service of Economy was traditionally predominantly involved in the setting of prices of medicines and implantable medical devices, it will now have to take on more responsibility with regard to the advertising of (online) healthcare products and services.

The interests of such non-healthcare agencies are from time to time at odds with those pursued by regulatory healthcare agencies. For example, considering the data protection concerns related to the transfer of personal data to certain countries, such as the US (see **10. Data Use and Data Sharing**), privacy experts generally recommend that personal data be kept as much as possible within the European Economic Area or any other country that has been recognised by the European Commission as offering sufficient safeguards for data protection. This suggestion does not only collide with the reality of global pharmaceutical or medical device companies, where much of the research and development (R&D) takes place in countries not offering adequate protection of personal data, but also conflicts with the requirements of regulatory agencies governing the authorisation and marketing of health products, which generally demand worldwide clinical and safety data.

The interplay between the responsibilities of non-healthcare and healthcare agencies is now more frequently uncovered and many regulatory agencies have made commitments to collaborate more closely with one another. It will now be important to ensure that these pledges are being put into practice and a harmonised regulatory framework is being established.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

Preventative healthcare (also referred to as "primary prevention") refers to a category of healthcare in which the main objective is to avoid a disease occurring by detecting health problems before any symptoms develop (eg, vaccination).

Diagnostic healthcare (also referred to as "secondary prevention") involves treating or diagnosing a disease as early as possible by monitoring existing problems, checking new symptoms, and following up on test results to initiate treatment without delay, and, as a result, reducing its mortality or severity (eg, radiology, ultrasound, cancer screening programmes and laboratory testing).

Preventative healthcare and diagnostic healthcare must be distinguished from curative care, which is only initiated when a disease has manifested itself with the onset of symptoms.

4.2 Increased Preventative Healthcare

The rapid convergence between digital technologies and healthcare has changed how preventative healthcare is delivered at the population level, shifting the focus from curative care to preventative care. New tools such as clinical decision support software, wearables, insideables, and fitness and well-being apps significantly contribute to actively monitoring a patient's health status and preventing or diagnosing diseases.

It is therefore not surprising that the future of healthcare is expected to be preventative, which is substantially cheaper (ie, diseases are prevented or diagnosed before they become major and expensive treatments are avoided) and is considered fundamental in the context of the future sustainability of the Belgian healthcare system.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Fitness and well-being apps that cannot be classified as a medical device (see **6. Software as a Medical Device**) are not (yet) regulated by the legislature. However, this does not necessarily imply that the data collected and processed through such apps is not regulated either. On the contrary, in the event that this data concerns information that is related to an identified or identifiable natural person within the meaning of the General Data Protection Regulation (GDPR), such processing must comply with the provisions of said regulation (see **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**). In addition, the EU funds an initiative (Label2Enable) that seeks to establish a high level of quality and reliability of health and wellness apps based on CEN-ISO/TS 82304-2.

4.4 Regulatory Developments

The use of mobile health apps in the healthcare process is becoming more common and plays a substantial role in the context of increased preventative healthcare (see **4.2 Increased Preventative Healthcare**). However, their reimbursement has long been a sore point in Belgium, particularly because of the difficulty of evaluating such apps. The Belgian federal government has therefore established a system making reimbursement of these apps possible. "mHealth-Belgium" is a platform that involves several stakeholders – including beMedTech, Agoria, the FAMHP, the eHealth-platform and the NIHDI – and centralises all relevant and necessary information regarding these apps for patients. It provides a validation pyramid consisting of three levels: M1, M2 and M3 (including M- and M+).

The first level, M1, requires that the CE mark is submitted and that the FAMHP is notified, which will then verify the app's conformity with the applicable medical device legislation. In addition to the requirements of the first level, apps entering the second level, M2, must meet all ICT requirements as imposed by the eHealth-platform in the context of cybersecurity and data protection and privacy. The third level, M3, regulates the funding and reimbursement of the app. In this regard, an app entering M3- is temporarily funded while still collecting data regarding its socio-economic value. If the app's socio-economic value is adequately proven, the app is eligible to enter M3+, which means that the NIHDI will officially reimburse the app. However, the rollout of the reimbursement pyramid has had limited success so far. Only one app, the rehabilitation and recover app "moveUP" has entered level M3- (meaning it is currently funded by the NIHDI while collecting the necessary data regarding its socio-economic value) and no apps have achieved level M3+.

As an alternative funding route, in order to promote sports and a healthy lifestyle, Belgian health insurance funds provide "additional advantages" such as partly reimbursing gym subscriptions or other (app) memberships. In addition, the NIHDI is strengthening the provision of psychological care for the Belgian population by largely reimbursing the costs involved. In this way, psychological care is becoming more accessible and the threshold lower. The Belgian e-Health Action Plan 2022-2024 also sets forth the ambition to integrate mental health care more comprehensively into care pathways to advance to a more holistic approach to healthcare.

4.5 Challenges Created by the Role of Non-healthcare Companies

The challenges non-healthcare companies might face – or that non-healthcare companies should at least consider – when entering the healthcare industry are extensive. Notably, this industry is highly regulated and complicated. Non-healthcare companies will therefore need to adjust their market strategies in accordance with the applicable regulatory frameworks that govern health products and services (eg, in the context of the promotion of medical devices). Moreover, these companies will also have to invest largely in compliance, which will very likely include compliance with data protection laws and regulations, intellectual property laws and regulations, and medical device legislation.

Finally, yet importantly, non-healthcare companies will need to take into account that they will have to accommodate not only the interests of the end users but also those of other stakeholders within the healthcare industry such as doctors, hospitals, health insurance providers and the NIHDI.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

The enhanced use of connected devices in healthcare can be explained by the confluence of societal and business challenges requiring increased reliance on tele- and digital health, and the development of advanced technologies enabling the same. The limited number of healthcare staff and constrained healthcare budget in Belgium necessitate a focus on cost-efficiency, which can be best achieved through value-based, personalised and remote healthcare. In addition, there is a clear desire on the part of patients to play a more active role in their treatment, by being able to consult their medical records through remote and mobile channels and by tracking their health data in real time through wearable devices.

IoMT devices (ie, digital healthcare products that connect to IT systems through online computer networks) have the potential to create a continuous stream of health data, making them the ideal solution for patient monitoring, diagnosis, patient support and intelligent decision-making. Cloud computing services can connect different devices, users and systems and are considered a convenient and efficient way to store and manage the massive amounts of data collected and processed. This enables interoperability between platforms, allowing patients and healthcare providers to easily access online health records which compile the patient's medical information from various sources. Finally, as discussed below (see **11. AI and Machine Learning**), AI-driven technologies may provide an array of benefits (and challenges) for healthcare providers and patients.

It is mainly through the integration of these technologies that a connected healthcare system can emerge, which not only optimises collaboration between healthcare providers (thereby reducing costs and increasing efficiency), but also enhances patient experience and control.

While the use of connected devices is rapidly gaining ground in all areas of healthcare, the follow-up of patients with chronic conditions (such as cardiovascular disease or diabetes) in particular has benefitted from the advances in remote monitoring. Women's healthcare has also been positively affected by the emergence of medical devices tracking, ao, ovulation, pregnancy and nursing. In addition to the vital role they play in remote monitoring and home (after-)care, IoMT devices such as smart beds, automatic nurse call systems and hand-hygiene monitors have the potential to increase efficiency and improve patient safety in hospitals.

5.2 Legal Implications

As discussed in detail hereunder (see **15. Liability**), in Belgium, the traditional regimes consist of contractual and extra-contractual liability. On top of that, Belgium's medical liability system is twofold, including the medical liability of a physician or a hospital as well as a fund to compensate for severe damage as a consequence of, for instance, medical accidents without liability. In this context, manufacturers, suppliers or sellers of health devices such as wearables, implantables and digestibles might be liable under the product liability framework if the end user (eg, a patient) has suffered damage due to the malfunctioning of such products. Given the upcoming extension of the product liability regime at EU level, the latter may become even more relevant.

5.3 Cybersecurity and Data Protection

The healthcare industry is particularly sensitive to data breaches and incidents (eg, the leaking of personal data) and cybersecurity attacks (eg, hacking). As a result, stakeholders should always carefully assess the possible implications and risks when making use of the IoMT, whether it be in a cloud computing environment or an on-premises and local computing platform. In the event that a digital healthcare company decides to collaborate with a cloud service provider, this service provider will likely process the data on behalf of the digital healthcare company. Within the context of the GDPR, the company might then be considered a controller (ie, which decides on the purposes and the means of the processing of personal data) and the service provider a processor, which, in turn, might outsource several processing activities to its sub-processors.

It is therefore of profound importance to contractually cover any risks relating to data protection and cybersecurity and to allocate the roles and responsibilities clearly and adequately in a data processing agreement. This agreement must include extensive audit rights for the benefit of the digital healthcare company as well as a liability clause that sufficiently protects the digital healthcare company in the event of any claims of patients or a data protection authority as a result of infringements by the cloud service provider. Lastly, the cloud service provider must ensure appropriate organisational and technical measures to secure any personal data and confidential documents stored.

Healthcare institutions making use of the IoMT should establish information security policies that encompass administrative, technical and physical safeguards to protect against the unauthorised or accidental disclosure, use, destruc-

tion, loss or alteration of patient information. These may include, for example, automated security testing tools and vulnerability scanners, cybersecurity training, spam blockers, the restriction of administrator privileges to a limited number of users, etc.

5.4 Proposed Regulatory Developments

The Belgian legislature is currently working on the transposition of the new Network and Information Security Directive or NIS2 (Directive (EU) 2022/2555), which entered into force on 16 January 2023 and replaces the first NIS Directive (Directive (EU) 2016/1148). NIS2 provides a better response to the growing threats posed by the digitalisation of healthcare and the surge in cyber-attacks through stronger security requirements, also addressing the security of supply chains, streamlined reporting obligations, more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the European Union. Since many hospitals and other healthcare providers in Belgium did not fall under the scope of application of the first NIS Directive, the NIS2 Directive will be particularly important for the Belgian healthcare industry as it extends the scope of entities to which the NIS requirements apply. According to the Belgian Centre for Cybersecurity, the total number of companies in Belgium covered by NIS legislation will increase by a factor of 20 to 40 with the introduction of NIS2. Belgium will have to adopt new provisions transposing NIS2 by 17 October 2024.

Meanwhile, the European lawmakers are putting the finishing touches on one of the recent years' most groundbreaking pieces of legislation intending to regulate artificial intelligence systems (see **11.2 AI and Machine Learning Data Under Privacy Regulations**), which will have an important impact in the field of the IoMT, to the extent the latter increasingly relies on AI-driven technologies.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Under the MDR, software is classified as a medical device in its own right (MDSW) if it is intended to be used for a medical purpose as set out in Section 2(1) of the MDR (eg, diagnosis, prevention, monitoring, treatment or alleviation of a disease, injury or disability, or control or support of conception). The medical device framework shall also apply if software is intended to drive or control the use of a medical device or can be considered as an accessory of a medical device. The classification of software as an MDSW has important consequences, as the medical device framework is complex and burdensome, especially for manufacturers that are just entering the digital healthcare market. Software companies may therefore be incentivised to indicate that their product is not intended for medical purposes and should instead be considered a fitness or wellness product, in order to avoid having to comply with this framework.

The MDR introduces a new risk-categorisation system for medical devices that entails that many MDSWs may now fall under Class IIA and higher. This may, for example, be the case when software is used to make therapeutic or diagnostic decisions (eg, clinical decision support software). If an MDSW cannot be classified under Class I, self-assessment will no longer suffice to receive the CE marking and, thus, market access for an MDSW may become increasingly time-consuming. Indeed, medical devices of Class II (A&B) and Class III must undergo a conformity

assessment procedure and (for certain Class IIB and Class III devices) a clinical evaluation before receiving the CE marking to be placed on the market. The same requirements apply to (software as) medical devices that use AI or machine learning. Moreover, the new draft regulation on AI (the "Artificial Intelligence Act" – see also **11. AI and Machine Learning**) recognises that medical devices powered by certain AI systems may be considered "high-risk" and proposes that the requirements for any such AI system should be checked in the conformity assessment of the medical device. As indicated above (see **2.2 Recent Regulatory Developments**), to the extent software is considered a medical device, it falls within the scope of authority of the FAMHP, which (as prescribed by the MDR), is responsible for designating and monitoring the notified bodies that carry out the conformity assessment procedure, and for the post-market surveillance of medical devices.

The MDR further requires that any proposed changes in the design, intended use, product-range, type or quality management system of a device are assessed and approved by the relevant notified body. Given that software improvements are made on a continuous basis, this requirement is ill-adapted to the reality of MDSW. The burden of undergoing an assessment procedure each time an update to the software is envisaged may effectively hold back improvements in patient care. The more rigorous requirements of the quality management system under the MDR compared to its predecessor and a focus on post-market surveillance in the MDR and the Artificial Intelligence Act are the first steps towards managing software that is improved or modified throughout its lifetime; however, a comprehensive framework on machine/deep learning medical devices is still absent and the current landscape still revolves around "static" rather than "dynamic" medical devices.

7. Telehealth

7.1 Role of Telehealth in Healthcare

Telehealth holds the promise of increasing the accessibility, efficiency and affordability of healthcare while offering the patient a more personalised and highly specialised approach. Through telehealth services, the patient's right to choose their physician is no longer determined by location but by best fit. In addition, telemonitoring services through wearables and other remote patient monitoring devices and technologies foster early discovery and intervention and provide physicians with a dynamic overview of a patient's health status as opposed to a snapshot at the time a patient comes in for consultation.

Tele-expertise is no longer limited to a select group of key opinion leaders consulting on rare diseases but is also readily used by general practitioners seeking advice from specialists.

Virtual hospitals (ie, healthcare facilities that operate completely online) could be a viable alternative to physical hospitals, especially for conditions that do not require urgent medical attention. Through the use of connected devices, audiovisual communication and AI, virtual hospitals would offer a solution to manage increased demand and costs, while also reducing patient exposure to infections.

Where hospitals and physicians go digital, the online (retail) pharmacy follows, providing pharmaceutical advice and products more rapidly and cost effectively. However, telehealth services also give rise to several risks and challenges, more notably regarding the credibility and certi-

fication of online healthcare providers; the confidentiality, privacy and security of patient data; the reimbursement of cross-border services; and medical liability.

7.2 Regulatory Environment

So far, Belgium does not have an integral telehealth framework. While telemonitoring and tele-expertise between physicians has been common practice for quite some time, the National Council of the Order of Physicians has long been opposed to diagnosing patients at a distance, asserting that considerable risks were involved and that, therefore, physicians could only diagnose patients without a physical consultation in exceptional cases. However, Directive 2011/24/EU on patients' rights in cross-border healthcare established the "country of origin" principle, meaning that healthcare professionals established in a member state of the European Union can provide healthcare services to patients located in other member states under the same terms and conditions as they are able to provide in their member state of establishment. In other words, Belgium cannot impose its regulatory framework on a healthcare provider that is established in another EU member state and is providing healthcare services to a recipient in Belgium. In addition, Directive 2011/24/EU obliges the NIHDI to reimburse certain cross-border healthcare services. This led to the contradictory situation where a patient could not receive reimbursed telehealth services from a physician located in Belgium, but that patient could receive (reimbursement for) those healthcare services if they were provided by a physician located in another EU member state.

The beginning of the COVID-19 crisis signified the end of an era in which healthcare was centred around in-person consultations and brought the telehealth framework on stream. The emergency measures taken by the legislature provided that telehealth services were allowed and were reimbursable by the NIHDI, if provided within certain conditions. However temporary these measures were, it is already apparent that the sudden widespread use of health services at a distance has induced a shift in mindsets, not only of physicians and patients, but also at the regulatory level. In a communication of June 2022, the National Council of the Order of Physicians has recognised that teleconsultations could be a valuable tool to complement face-to-face patient care, under certain conditions. Notably, precautions must be taken to guarantee the quality and continuity of care, such as updating the patient's electronic record, and the therapeutic relationship between the patient and the physician (including the consent of the patient) must be adequately established. Further, physicians should only prescribe medicinal products or medical devices via Recip-e, the official system for electronic prescriptions. The National Council has, since its communication in June 2022, advised on a number of topics relating to teleconsultations, including whether a certificate of absence can be provided to a patient by its physician during teleconsultations without face-to-face contact and whether a deposit for booking a doctor's appointment via a platform can be requested.

Slowly but surely, a liberalisation on the sale of medicines and medical devices is also emerging. As of 2019, patients and healthcare professionals can purchase their medical devices (carrying a CE mark) directly (online) from any distributor or manufacturer instead of in a pharmacy.

Since remote healthcare, logically, relies heavily on the use of online platforms enabling audiovisual communication, the EU Digital Services Act, which came into force on 16 November 2022,

and will apply as from 1 January 2024, will have a significant impact as well.

7.3 Payment and Reimbursement

Telehealth services have only been introduced in the nomenclature of the NIHDI in the past few years and, even now, a comprehensive reimbursement scheme is lacking. Certain mobile health applications that (i) are classified as a medical device, (ii) are CE marked, connected or interoperable with the Belgian eHealth-platform, and (iii) have demonstrated sufficient socio-economic added value are eligible for reimbursement. In April 2022, for the first time in Belgian history, the NIHDI decided that a recovery and rehabilitation app (a DTx product) could receive preliminary funding while a rolling review on the socio-economic value of the app was ongoing (see **4.4 Regulatory Developments**).

Finally, as of August 2022, teleconsultations via video or telephone conference are included in the nomenclature of the NIHDI and consequently reimbursed. The NIHDI is also testing a number of pilot projects concerning telemedicine and has expressed its commitment to develop a consolidated framework in the near future.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

Consumer and connected devices and the IoMT are welcome allies in the fight against a rise in welfare and chronic diseases, the challenges arising from an ageing population and a healthcare budget that is increasingly under pressure from innovative but high-cost therapies. As discussed above (see **5.1 Internet of Medical Things and Connected Device Environment**), it is mainly the integration of different technologies such as cloud computing services, AI-driven and machine learning technologies and sensor tag technology in (wearable) devices connected to mobile applications that has enabled the IoMT to flourish. Through wearables, physicians can monitor patients consistently and effectively at home, leaving hospital beds available for patients who need to be admitted for intervention. The older generation is able to live at home for a longer period via the help of digital assistants and medical-alert systems, which reduces the burden on residential care centres and care staff. Lastly, individuals are empowered to take their health into their own hands and, consequently, the overuse of healthcare services is prevented.

Nonetheless, the devices and applications related to the IoMT are not without their controversies. To begin with, mobile health applications and consumer devices are often presented as a wellness or fitness device and manufacturers avoid labelling their products as “intended for medical purposes” in order to evade the stringent regulatory requirements applicable to medical devices (for more information on classification as a medical device, see **6. Software as a Medical Device**). Accordingly, medical advice may be disguised as lifestyle recommendations given by unqualified professionals, contrary to the rules on lawful practice of medicine and the regulatory oversight by the FAMHP on medical devices.

Another key problem is the inequality of access to these devices and technologies, as the reimbursement schemes for digital healthcare applications remain fragmented (see also **7.3 Payment and Reimbursement**). Furthermore, since the patient data collected by IoMT devices and applications is often transmitted to the manu-

facturer prior to being provided to the healthcare provider, the medtech industry collaborates with healthcare professionals more closely and comes into contact with patients and patient organisations more often and more closely, which results in concerns regarding the advertising and promotion of health products. Last but not least, cybersecurity and privacy risks (eg, cyberattacks, malware, data breaches, phising, etc) are also prominently present in this field of digital healthcare, as devices, technologies and applications are interconnected, which increases the "attack surface" of healthcare organisations and complicates the monitoring of security vulnerabilities. This lack of visibility also affects the security of personal (health) data collected in this setting, which is processed outside the strict realms of healthcare provision.

To date, the increased security risks resulting from the integration of different technologies and the connectivity between devices remains insufficiently addressed by applicable cybersecurity and data protection legislation and policies. However, the importance of ensuring device security in a healthcare setting cannot be underestimated, especially since any alterations in the functioning of IoMT devices resulting from cyberattacks could potentially jeopardise a patient's life. While it is the responsibility of device manufacturers to design security and data protection into their devices, healthcare organisations could also take protective measures; eg, by creating an isolated network for connected devices, investing in the automated monitoring of security vulnerabilities and organising cybersecurity training for their staff.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

The low latency, increased speed and bandwidth of 5G networks allows cellular wireless networks to compete fully with wired networks in the provision of digital healthcare. This, in turn, could allow for the provision of telehealth services from, and to, practically everywhere, even in the absence of wired networks. The possibilities for remote healthcare that 5G brings to the table are crucial for medical treatment in disaster areas, as wired infrastructure might be impacted or destroyed as a result of a disaster, or these areas might be hard to reach. The same applies for first responders, who, through 5G technology, will be able to provide remote first aid or benefit from the qualities and experience of specialists and colleagues without a need for their physical presence.

Moreover, the aforementioned qualities of 5G networks coupled with its increased connection density will allow for a more complete and effective integration of technologies such as the IoMT in digital healthcare. For example, one might think of the use of sensors and wearables, allowing the monitoring of vital functions not only during a telehealth consultation but consistently over a longer period, providing healthcare practitioners with useful insights on the overall health, stability or pathology of a patient. The use of IoMT technologies (enabled by 5G networks) will allow this data to be transmitted automatically to healthcare practitioners and allows the various wearables or sensors to communicate and interact with each other.

Overall, it can be expected that 5G will enable the provision of remote healthcare services in a more effective, reliable and comprehensive man-

ner, with the possibility of remote operations due to low latency of 5G networks as a pinnacle.

Nonetheless, the highly sensitive and private nature of data created, processed and transferred in the context of digital healthcare is diametrically opposed to the public character of (5G) wireless communication networks. Hence, when entering into arrangements with telecoms providers that deploy and manage a 5G network, sufficient attention to provisions regarding responsibility for network security and data protection and privacy will be paramount. Furthermore, when relying on (wireless) technologies for the provision of critical services such as healthcare services, contractual provisions regarding the assurance of connection stability and liability for failure or interruption of services will also be crucial.

In the Belgian context, it needs to be noted that the telecom sector is currently an enforcement priority of the Belgian Competition Authority, which became evident when the Authority announced that it launched an investigation into anti-competitive practices in the roll-out of fibre-optic networks. The outcome of such investigation may further impact the roll-out of such networks and consequently, the 5G connection that may depend upon them.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

Patients have the right to privacy and a carefully kept and stored patient record in relation to their healthcare professional (Articles 9 and 10 of the Act of 22 August 2002 on Patients' Rights and Articles 33–40 of the Health Care Quality of Practice Act of 22 September 2019). However, the time when medical confidentiality by healthcare professionals was sufficient to safeguard patients' health information is long gone. Patient information is currently stored in an electronic health record on the eHealth-platform and can, to the extent relevant for treatment, be accessed by a patient's healthcare provider after having obtained that patient's consent. In addition, in a digitalised healthcare industry, several other participants will need to process a patient's personal data. Personal information regarding health and genetic and biometric data (for the purpose of identification) is considered sensitive personal data under Article 9 of the GDPR. Processing of such personal data is principally prohibited, unless a justification applies. Personal data relating to health can therefore only be processed in exceptional cases.

Besides the GDPR, recent initiatives have been taken to empower the patient in taking a more active role in the management of their health and accompanying health data. For example, under the recent proposal to amend the Patients' Rights Act of 22 August 2002, the patient is able to record some of its choices (eg, with respect to its care plan) online and its right to receive information about its health status is reinforced.

Implications of Schrems II

Data protection in the healthcare industry is further complicated by recent developments. The landmark Schrems II case of the European Court of Justice quashed the EU–US Privacy Shield and questioned the validity of data transfers under the (old) European Commission's standard contractual clauses (SCCs) to third countries with inadequate data protection and privacy laws. In response, the European Commission issued modernised SCCs on 4 June 2021. Nevertheless, the question as to whether

these transfer mechanisms are sufficient to overcome inadequate data protection and privacy laws in third countries remains unchanged, in particular considering recent decisions of data protection authorities involving large tech corporations in the US. This is a significant hurdle as (med)tech companies are often global enterprises and innovative health solutions require collaborations across borders. If (health) data can no longer be transferred to tech-savvy countries such as China and the US (regardless of the safeguards taken by contracting parties), this may drastically impair digital healthcare progress. In this respect, it needs to be noted that the European Commission has adopted an adequacy decision for US companies participating in the EU-US Data Privacy Framework as recently as July 2023, which should considerably facilitate transfers to the US in a commercial context. It remains to be seen whether this new framework will withstand a scrutiny test by the Court of Justice of the European Union, contrary to its predecessor.

Data Processing in Partnerships and Secondary Use

Other uncertainties relate to the data processing roles and responsibilities in multi-stakeholder innovative partnerships such as consortium agreements, but even in multi-study-site clinical research projects, it remains dubious which processing role each party takes on. This leads to ambiguity for data subjects and can cause considerable delays in negotiations in partnership agreements.

Another point of interest is the possibility to use existing research data for secondary use. The GDPR and the European Commission guidelines provide some flexibility to ask for consent for a broader field of research instead of for one research project; however, it remains to be seen how any such margin should be interpreted in practice (see Recital 33 of the GDPR).

In Belgium, legislative steps have been taken to establish a health data authority to, amongst other objectives, supervise secondary (research) use of health data.

European Health Data Space

In closing, the European Commission is currently working on an ambitious project that would constitute a European Health Data Space, holding qualitative health data and facilitating the sharing of data for research, innovation and improvement of public health without losing sight of data protection and privacy. If this initiative were to succeed and were to gain the trust of patients and healthcare providers, the path forward for machine learning, AI, research and innovation may look quite promising.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

In the current healthcare ecosystem, it may be more appropriate to make use of the term “augmented intelligence” rather than “artificial intelligence”; that is to say, human capabilities can only be augmented but not replaced by intelligent devices. AI systems work well in verifying outcomes, correcting human errors and processing large amounts of information efficiently, but are presently not intended to function without human instruction, oversight and intervention in an industry as sensitive as the healthcare industry.

AI-driven technologies could offer an automated analysis of the collected data, recognising or

predicting diseases to significantly increase the quality and speed of diagnosis.

For machine/deep learning and AI to work to the best of their abilities, large amounts of highly qualitative training data sets are needed. This requirement seems often to be at odds with a few of the basic principles of the GDPR, such as purpose – and use – limitation and data minimisation. It may therefore be challenging to secure sufficiently comprehensive rights on data in order to be able to use and share such data with relevant partners. Transparency and patient empowerment are useful tools that may help this purpose; ie, if extensive information about the processing of personal data is given by the healthcare provider to the patient, a patient is more willing to give its free informed consent (although the adequacy of consent as a legal basis must not be overestimated).

Lastly, due to the emergence of virtual assistants (such as Alexa), natural language processing (NLP) (ie, the ability of a computer program to understand human language as it is spoken and written) is slowly but steadily becoming integrated into the healthcare industry. However, NLP has led in the past to significant concerns from a data protection and privacy perspective due to the difficulty to confirm and verify the results of the data processed by AI systems, which are often characterised by bias. As a result, AI is usually difficult to deploy in a transparent manner and thus it is paramount to always carefully assess its intended use (eg, data processing impact assessment) in order to apply appropriate additional measures.

11.2 AI and Machine Learning Data Under Privacy Regulations

In April 2021, the European Commission unveiled its AI package proposing new rules and actions to turn Europe into the global hub for trustworthy AI, including a proposal for a European regulatory framework on AI, the so-called Artificial Intelligence Act, which is currently moving through the legislative process (the European Parliament adopted its position, including several amendments in June 2023). Although the Artificial Intelligence Act aims at protecting fundamental rights when AI is deployed, it does not cover any risks relating to black box AI nor are there any guidelines in place that apply to this concern.

Due to the lack of transparency, black box AI poses a significant challenge in the context of the processing of personal data. Namely, data subjects (eg, patients) have the right not to be subject to a decision based solely on automatic processing (Article 22, GDPR). A data subject may therefore request that a decision made about them by automated means shall be reviewed by a natural person (eg, a doctor). It may be difficult for the natural person to assess whether the decision made by an AI system was correct if that person is not aware of how the AI system decided on a certain outcome.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Companies that are entering the digital healthcare market by developing and selling new digital healthcare technologies should be aware of the challenges that the convergence of two industries entails. Traditional healthcare or pharmaceutical companies may be confronted with pertinent challenges relating to cybersecurity and data protection when entering digital markets (eg, ransomware, phishing and denial-of-service attacks). On the other hand, companies that are ordinarily involved in the offering of

digital services and products to customers may be surprised to learn about the highly regulated context of the healthcare industry and the additional compliance requirements associated with entering that market.

Healthcare institutions or other customers of such new technologies have every interest in appropriately allocating the roles and responsibilities when negotiating agreements (eg, master services agreements, software as a service (SaaS) agreements and data processing agreements) and in adequately addressing any inherent risks.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

In order for digital healthcare to be fully embraced by healthcare organisations and healthcare professionals, considerable changes to the infrastructure and organisation of hospitals and practitioners will be required. For instance, several cyber-attacks on Belgian hospitals and testing centres during the COVID-19 crisis have proven that healthcare institutions are a frequent target for cybercriminals and are often ill prepared for such a challenge.

At the level of the individual practitioner, several barriers prevent the adoption of healthcare technologies. A study by the Belgian Health Care Knowledge Centre concluded that general practitioners struggle with security concerns and an overload of information on e-health platforms. They also have to invest substantial amounts of their own time in getting to know new IT systems and they are reluctant to depend on external services for the operability and functioning of their general practice.

Besides investment in better infrastructure, due care should be given to a radically different manner of educating healthcare providers. In order for AI, mobile health technologies and wearables to find their way to individual practitioners, these caregivers should be incentivised and educated thoroughly and continuously. The Health Care Quality of Practice Act of 22 September 2019 imposes an obligation of continuous learning on healthcare professionals; however, multiple implementing acts are still required and qualitative digital healthcare learning opportunities need to be offered to practitioners.

As a final point, while improving the infrastructure at the level of healthcare organisations and professionals is critical for advancing digital healthcare, careful consideration should also be given to equal access and non-discrimination of patients. The uptake of the IoMT and general connectivity of patients must therefore also be reviewed on a population level.

13.2 Data Management and Regulatory Impact

Data management is of the utmost importance for companies active in the healthcare industry. For instance, adequately managing clinical trial data is fundamental with regard to the set-up, conduct and successful outcome of clinical trials. In this context, the Clinical Trial Regulation (Regulation (EU) No 536/2014) regulates clinical data management, which should result in the generation of high-quality and statistically reliable data from clinical trials. The central database "Clinical Trials Information System" supports the entry, verification and quality control of data collected during clinical trials.

As discussed (see **13.1 IT Upgrades for Digital Healthcare**), the healthcare industry is a frequent target for cyber-attacks, and is generally

ill prepared for such hazards, requiring swift and appropriate measures. In this context, there are several national and European initiatives, laws and regulations that aim at fostering and upgrading companies' IT infrastructure and ensuring the continuity of care, including the Early Warning System of the Belgian Centre for Cybersecurity, the (anticipated Belgian implementation of the) NIS2 Directive or the Health Care Quality of Practice Act of 22 September 2019.

Importantly, several initiatives have been launched to improve the sharing of (both personal and non-personal) data on the EU level, including by means of the Data Act and the Data Governance Act.

14. Intellectual Property

14.1 Scope of Protection

There are no frameworks in place that particularly apply to the protection of intellectual property in the field of digital healthcare. Therefore, one has to revert to existing and traditional regimes regarding intellectual property protection. Slowly but steadily, those regimes are being updated to keep pace with rapid technological developments.

Inventions are patentable if they fulfil the criteria of novelty and inventiveness and if they are capable of industrial application. Computer programs are in principle exempt from patent protection as such; however, software may be protected if incorporated in a product of a technical nature. Problems arise in relation to the inventor of AI inventions. Under the current guidelines for applications to the European Patent Office, the inventor needs to be a human being. This is problematic when inventions are made by AI without human intervention. In addition, one might wonder whether patents for inventions made by AI need to be vested in the researcher who discovers the invention when using the AI technology, the owner of the AI technology or the developer of that technology.

Furthermore, the author of a literary or artistic work that is original and expressed in a specific form is granted copyright protection. To the extent software and databases meet the requirements of expression and originality, they can also be protected by copyright. Copyright only protects the structure of a database and not its content. In addition, the content of a database can be protected by the Sui Generis Database Right if the acquisition, control or presentation of that content qualitatively or quantitatively represents a substantial investment on the creator's or developer's part (Article XI.306 of the Code of Economic Law). The European Union Directive 2019/790 on Copyright and Related Rights in the Digital Single Market (the Copyright Directive), which has been transposed into Belgian law by the Act of 19 June 2022, attempts to make the copyright legal framework more adapted to the reality of the digital environment in which works are now created, distributed and exploited.

Trade secret protection in Belgium is detailed in Title 8/1 of Book XI of the Code of Economic Law and based on Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Information constitutes a trade secret if:

- it is not generally known or readily accessible to persons in circles that normally deal with the kind of information in question;
- it has commercial value because of its secrecy; and

- it has been subject to reasonable steps to keep the information secret.

The illegitimate disclosure or acquisition of such information can be contested in court and sanctioned.

14.2 Advantages and Disadvantages of Protections

There are many advantages and disadvantages in the context of intellectual property protection. A pertinent example relates to the fact that such protection might simultaneously foster and hinder innovation.

On the one hand, intellectual property protection plays a crucial role in fostering innovation, particularly in the context of R&D. Digital healthcare companies invest heavily in the development of a product, which usually requires a lot of time, energy and money. Successful products might be highly lucrative, which, in turn, might result in the digital healthcare company having a commercial advantage when compared to its competitors. Therefore, once granted, intellectual property protection provides the necessary tools to safeguard the hard work and prevent competitors from infringing the product. In this context, intellectual property incentivises innovation.

On the other hand, intellectual property protection might hinder innovation, especially when digital healthcare companies seek to obtain intellectual protection solely for anti-competitive purposes and hence use this protection to prevent competitors from entering the market. For instance, the digital healthcare company might use patents as a strategic deterrent by building up so-called patent thickets, making follow-on innovation by other firms entering the market a more challenging, costly or even impossible process.

The latest regulatory developments at EU level endeavour to address this tension by striking a balance between the advantages of intellectual property protection on the one hand and the need to make data more accessible to stimulate data-driven innovation on the other.

In this context, a noteworthy example of the merits of the Copyright Directive would be the introduction of exceptions to copyright for text and data mining (ie, the automated analysis of large bodies of data in order to generate knowledge on patterns, trends and correlations), which will be particularly useful for the training of data-driven AI systems. Indeed, having to obtain the prior authorisation of the owner of a database before being able to extract data from it would be excessively time consuming in the context of the development of an AI system.

Additionally, the European Commission's proposal for a Data Act will likely have an impact on different forms of intellectual property protection. It provides, for example, that the Sui Generis Database Right (discussed above) does not apply to databases containing data obtained from or generated using an IoT product or related service. The absence of intellectual property protection for the content of such databases will significantly facilitate the use and sharing of (health) data resulting from IoMT devices. The proposal further seems to provide exceptions to the rule that trade secrets should only be disclosed with permission of the holder, as part of the data sharing obligations it introduces. However, the proposal also shows respect for intellectual property rights by expressly requiring that any such disclosures are backed by confidentiality obligations and clarifying that the

obligation of the holder to make data available to a data recipient does not automatically oblige the disclosure of trade secrets, unless otherwise required by EU or national law.

14.3 Licensing Structures

The contractual licensing structures in the digital healthcare industry vary depending on the type of product. For example, to download medical, fitness and well-being apps, digital health providers will usually offer an end-user licence agreement in order for the end user (B2C) to be able to use the app and its underlying software. As far as it concerns the licensing of cloud services, generally, the SaaS licence is used, where the cloud service provider hosts the app and related data, and makes it available to end users (B2B and B2C) over the internet.

14.4 Research in Academic Institutions

Education is a competence of the Communities in Belgium. The Codex Higher Education of the Flemish Community provides that the intellectual property rights to inventions created by salaried researchers in the course of their research duties for the university or the university of applied sciences are vested in that university (of applied sciences). The university has the sole right to exploit any such inventions. Belgian universities have a long tradition of creating and supporting spin-off companies and the Flemish Catholic University of Leuven (KU Leuven) has been named the most innovative university in Europe several years in a row for its large amount of (successful) patents filed in the field of pharmaceuticals and biotech, agriculture and food, chemicals and medical devices.

Belgian universities often collaborate with industry partners and participate in European consortium projects by conducting R&D or seconding one of their researchers to a project. The ownership and exploitation of intellectual property rights differ from project to project; however, Belgian academic institutions often endeavour to secure the ownership rights to their R&D results and grant the exploitation rights to the industry.

14.5 Contracts and Collaborative Developments

The pandemic has evidenced that better public health is driven by improved collaborative working, including through public-private partnerships. In order to foster the innovation that such partnerships can yield, trust between the different participants needs to be built, including while drafting and negotiating R&D agreements. In this regard, the allocation of ownership and exploitation rights for digital health inventions must be determined from the outset.

As previously stated, default statutory rules vest intellectual property rights of new ideas, works or inventions with the inventor or author of such work. Therefore, pharmaceutical and medtech companies that outsource part of their R&D need to consider which rights they need to secure in relation to the results of the R&D, including if, and to what extent, they have sufficient freedom to operate to exploit the outcomes of their research investment commercially.

15. Liability

15.1 Patient Care

New technologies increase the number of participants involved in healthcare and make it increasingly complicated for a patient to seek redress for damage caused in the provision of healthcare. The liability of a physician or hospital can be invoked contractually and extra-contractually, depending on the act from which the

damage arises. Furthermore, patients can seek compensation from the Fund for Medical Accidents in the case of severe damage caused by:

- medical accidents without liability;
- medical accidents with liability where the healthcare provider's insurer disputes the liability or makes a manifestly inadequate proposal; and
- medical accidents with liability when the healthcare provider is not insured or is inadequately insured.

This Fund for Medical Accidents is financed exclusively by the Belgian state and is a service of the NIHDI.

Furthermore, product liability for medical devices is based on the strict liability regime of Directive 85/374/EEC. In this regard, a medical device is defective when it does not provide the safety that a person is entitled to expect, taking into account all circumstances, including:

- the presentation of the product;
- the reasonably expected use of the product; and
- the time when the product was put into circulation.

Any person in the production chain, the EU importer and the supplier might be held liable.

In light of new technologies, these classic liability regimes may need to be revisited. A first step has already been taken by the EU Digital Services Act, which (slightly) updates the rules on liability of providers of online intermediary services, including cloud services providers, in relation to illegal content provided by the recipient of the service and published on the online platform. While the liability of the provider for copyright breaches and other infringements committed by customers through their services remains limited in principle, the EU Digital Services Act introduces more extensive transparency and due diligence obligations, which may result in an increased risk of liability for the provider. This may have implications for hosting service providers involved with health data and/or intermediaries connecting patients with HCPs.

AI-driven software sometimes lacks transparency in its decision-making and demonstrates considerable autonomous behaviour. This leads one to question whether a physician is at fault (and liable) if that physician does not follow a diagnosis made by an AI technology or, conversely, whether that physician fails to perform the required due diligence by making treatment decisions based on a diagnosis made by an AI technology without knowing exactly how the software reaches a conclusion.

With respect hereto, the new legislative proposal of the European Parliament on AI suggests the implementation of both a strict liability and a fault-based liability regime for AI technologies, depending on the risk involved in that AI system. Similarly, the Product Liability Directive may not always offer relief with regard to defects in digital health technologies, as many of these applications contain one or several service elements, which may make it more difficult to classify the technology as a defective product.

Finally, the EU is currently overhauling its product liability laws in an attempt to better address the risks resulting from the new technological developments. The most important changes proposed include the expansion of the definitions of "product" to include software and "defect" to include cybersecurity and connectivity issues; the expansion of the scope of the damages that

can be claimed to include data loss or corruption; the removal of the EUR500 threshold for claims and the reduction of the burden of proof for scientific or technically complex cases. It is clear that these updates will have a significant impact on life sciences companies, especially those developing IoMT devices and other digital healthcare solutions.

15.2 Commercial

As stated above, multi-participant involvement in the manufacture of digital healthcare technologies and the provision of healthcare services has made it gradually more complex to allocate responsibility. Under the defective product regime, any participant in the supply chain may be held liable, including the EU importer and the supplier.

As with data protection, any controller is accountable for any damage that arises from a processing activity that breaches the GDPR, in contrast with processors, which are only responsible for damage that is the result of that processor acting outside the lawful instructions of the controller. Data processing agreements thus often include rigid liability and indemnification obligations to ensure a controller can recover the damage that is caused by its service provider from that processor.

CHINA

Law and Practice

Contributed by:
Alan Zhou, Charlene Huang, Jenny Chen and Sylvia Dong
Global Law Office

Contents

Global Law Office was one of the first law firms in the People's Republic of China (PRC), with more than 600 lawyers practising in its Beijing, Shanghai, Shenzhen and Chengdu offices. Its life sciences and healthcare (L&H) practice group, also known as China Life Sciences & Healthcare Law (CLHL), is one of the leading advisers in China, having provided "one-stop" legal services for every sector of the L&H industry, including R&D, clinical research organisations, pharmaceuticals, biotechnology, medical devices, supply producers and distributors, hospitals and other healthcare providers and investment funds. GLO advises clients on challenging L&H legal issues such as regulatory compliance, structuring transactions and contractual arrangements, realisation of pipeline and geographic expansions, capital-raising and project-financing, M&A, reorganisations, IP protection, licensing and distribution arrangements, settlement of disputes involving adverse effects in clinical trials and medical treatment. The firm has close links to industrial associations and makes recommendations on industry codes of conduct and compliance management standards.

Authors

Alan Zhou is the head of life sciences and healthcare (L&H) practice of Global Law Office and the head of China Life Sciences & Healthcare Law (CLHL). He has been recognised as a pioneer in providing outstanding legal consulting services in the L&H practice. Alan has routinely represented multinational corporations, well-known Chinese state-owned and private enterprises, and private equity/venture capital funds in the L&H area. He has been engaged by local authorities and industrial associations to advise on legislation and industrial standards in the L&H industry, areas of which include e-healthcare, medical insurance reform, medical representative administration, and other compliance issues. He has won numerous awards and has been recognised by peers for his expertise, and is widely published both in China and internationally.

Charlene Huang is a partner based in Global Law Office's Shanghai office, with in-depth experience in M&A and cross-border licence deals, especially in the sector of healthcare and life sciences. She has led projects involving outbound and inbound investment, acquisition of state-owned and private equity/assets, pipeline consolidation or restructuring of MNCs, and various licence or collaboration deals in the pharmaceutical, medical device and medical services sectors. She regularly provides support and advice on projects concerning cell therapy, gene therapy, digital healthcare, medical AI, etc. Charlene also has in-depth experience advising multinational companies in general corporate, cybersecurity and data management.

Jenny Chen is an of counsel in Global Law Office based in Shanghai, an attorney at law in the PRC, a certified fraud examiner of US ACFE, a certified public accountant (non-practising), and passed the US California Bar Exam. She focuses her practice on compliance, government investigation, internal investigation and data security. Jenny is well versed in conducting investigations in connection with anti-corruption (US FCPA and UK Bribery Act), financial frauds, occupational embezzlement, self-dealing and trade secrets. Jenny has extensive experience in cybersecurity and data compliance. She has handled multiple large-scale projects in e-discovery, cross-border data protection and security, and sensitive information review.

Sylvia Dong is an of counsel in Global Law Office based in Shanghai, an attorney at law in the PRC, and admitted to practice in New York State, USA. Her main practice covers M&A, PE/VC and capital markets, and she is especially focused on the life sciences industry and the TMT industry. She has rich experience in investment, licence deals, business collaborations, general corporate and compliance in the industry of life sciences and healthcare. She also represents well-known healthcare and telecommunications companies handling digital projects.

Global Law Office

35th & 36th Floor
Shanghai One ICC
No.999 Middle Huai Hai Road
Xuhui District
Shanghai 200031
China

Tel: +86 21 2310 8200
Fax: +86 21 2310 8299
Email: Alanzhou@glo.com.cn
Web: www.glo.com.cn

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Digital healthcare, digital medicine and digital therapeutics are not legal terms defined in People's Republic of China (PRC) laws and regulations, but are frequently referred to in commercial contexts and industry policies.

Digital healthcare usually refers to healthcare technologies developed based on information technologies used by and for the public in general, including:

- healthcare management;
- disease awareness;
- telemedicine;
- online sale of pharmaceutical products; and
- other healthcare-related activities conducted through digital platforms.

Digital medicine usually refers to the application of information technology in the process of diagnosis and treatment, which can only be performed by qualified medical institutions.

Digital therapeutics usually refers to the software-based products that are used for therapeutic interventions, either as monotherapy or in combination with other conventional medical therapies. Such products usually fall within the category of medical devices, and therefore are subject to regulatory administration to ensure their safety and efficacy.

1.2 Regulatory Definition

As previously stated, digital healthcare, digital medicine and digital therapeutics are not legal terms defined in PRC laws and regulations, but are frequently referred to in commercial contexts and industry policies. Nevertheless, should any service or product in the fields of digital healthcare and digital medicine fall within the category of pharmaceuticals or medical devices, or be used for the diagnosis and treatment of human diseases, administrative regulations would correspondingly apply.

1.3 New Technologies

Given the broad application scope of key technologies and the fact that digital healthcare and digital medicine are sometimes used interchangeably in practice, it would be difficult to accurately distinguish between the two fields.

Generally speaking, for digital healthcare, key technologies may include:

- big data that can be used in public health monitoring;
- healthcare cost control; and
- the internet of things and related sensor technology, global positioning system (GPS) technology and 5G technology that enables smart home and elder care, hospital management, telemedicine, etc.

For digital medicine, key technologies may include artificial intelligence (AI) and machine learning used for assisted diagnosis and treatment, medical imaging, etc.

1.4 Emerging Legal Issues

Key emerging legal issues in digital health may include the following.

Regulatory Framework

Digital healthcare activities, based on different scenarios, are governed by:

- PRC physician practising laws and telemedicine-related regulations;

- PRC drug administrative laws and regulations in relation to online sale of pharmaceutical products;
- PRC advertising laws;
- PRC laws and regulations on cybersecurity and data protection; and
- PRC laws, regulations and industry standards on telecommunications and information technology.

However, a unified and systematic law or regulation to specifically govern the digital healthcare industry is still under development.

Cybersecurity and Data Protection

As digital health involves a large amount of personal data, especially that of a sensitive nature, the design and implementation of life-cycle protection of such data needs to be carefully considered, under the cybersecurity and privacy protection laws and regulations – especially regulations of the PRC Personal Information Protection Law that came into effect on 1 November 2021.

Liability

As AI technologies are more frequently used in diagnosis and treatment by healthcare institutions, in circumstances where personal damages are caused to patients due to the application of such technologies, which party should assume responsibility needs to be further analysed.

1.5 Impact of COVID-19

The demand for digital healthcare technologies and healthcare services has grown significantly during the COVID-19 pandemic.

Prior to the outbreak of COVID-19, most patients in China typically visited physical healthcare institutions such as public hospitals, private hospitals or clinics. However, due to the restriction on movement necessitated by the pandemic, a series of notices and opinions were issued to encourage healthcare institutions to leverage telemedicine for the purpose of relieving the pressure on the offline delivery of healthcare services and ensuring COVID-19 patients' timely receipt of diagnosis and treatment.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

The authorities involved in the regulation of digital healthcare technologies mainly include the following, at a national level, and their subordinate branches as applicable.

The National Medical Products Administration (NMPA)

The NMPA regulates drugs, medical devices and cosmetics in China, and is responsible for their safety supervision and management, from registration and manufacturing to post-market risk management. Technology and devices, including software that falls within the category of a drug or medical device, are also subject to regulation and supervision by the NMPA and its subordinate branches.

The National Health Commission (NHC)

The NHC primarily formulates and enforces national health policies and regulations pertaining to healthcare institutions, healthcare services and healthcare professionals (HCPs). Internet-based diagnosis and treatment (including internet hospitals) and remote consultations between healthcare institutions and patients are both regulated by the NHC.

The clinical application of medical technologies for the purpose of diagnosis and treatment

(including AI-assisted diagnosis and treatment) by healthcare institutions and professionals is also regulated by the NHC.

The National Healthcare Security Administration (NHSA)

The NHSA is primarily responsible for implementing policies related to basic medical insurance (BMI), such as reimbursement, pricing and the procurement of drugs, medical consumables and healthcare services.

2.2 Recent Regulatory Developments

Regulatory Developments on Telemedicine

"Internet Plus Healthcare" – ie, healthcare in combination with application of the internet – is now a key national strategy in China. In order to regulate diagnosis and treatment provided remotely – ie, teleconsultation by HCPs or internet-based diagnosis – in July 2018 the NHC and the National Administration of Traditional Chinese Medicine issued:

- the Administrative Measures for Internet-based Diagnosis (for Trial Implementation) (the "Internet-based Diagnosis Measures");
- the Administrative Measures for Internet Hospitals (for Trial Implementation) (the "Internet Hospital Measures"); and
- the Good Practices for Telemedicine Services (for Trial Implementation) (the "Rules on Telemedicine").

Furthermore, the NHC and the National Administration of Traditional Chinese Medicine released the Rules for the Regulation of Internet-based Diagnosis (for Trial Implementation).

These measures clarify how teleconsultation and internet-based diagnosis should be carried out and set forth the regulatory requirements thereof.

In addition, the growth of internet-based diagnosis also boosted the demand for internet sales of medicine. Currently, with the Provisions for Supervision and Administration of Online Drug Sales newly enacted on 1 December 2022, except for medicinal products subject to special administration, internet sales of both over-the-counter drugs and prescription drugs are allowed.

Regulatory Developments on Electronic Medical Insurance

In August 2019, the NHSA issued the "Internet Plus" Medical Service Prices and Medical Insurance Payment Policy and launched the electronic medical insurance system, which regulates prices and insurance policies to allow for internet-based healthcare services to be covered by China's medical insurance system. Implementation policies were further issued in 2020 and local enforcement rules have been gradually issued by local authorities since 2021.

Regulatory Developments on AI-Assisted Diagnosis and Treatment

In February 2017, the NHC issued updated administration regulations on both AI-assisted diagnosis technology and AI-assisted treatment technology, together with the applicable quality control criteria for clinical application, reflecting the most recent regulatory position of the NHC to encourage, while strictly regulating, the development and cybersecurity application of AI-assisted diagnosis and treatment for safety considerations.

In 2019, the NMPA issued the Key Considerations for Review of Medical Device Software Using Deep Learning Technology for Assisted Decision-Making, laying out its concerns for registration review of the relevant medical device software, including software development, soft-

ware updates and related technical considerations. In 2021 and 2022 respectively, the NMPA issued the Guiding Principles for the Classification and Definition, and the Guiding Principles for Registration Review of AI Medical Devices, the latter laying out the application requirements and technical review standard of AI medical devices. In 2022, the NMPA issued a series of industry standards related to the quality requirements and evaluation of AI medical devices.

Regulatory Developments on Data Protection

In July 2018, the NHC issued the Administrative Measures on the Standards, Security and Services regarding National Healthcare Big Data (the "Measures on Healthcare Big Data"), announcing the direction of regulating the use and application of the healthcare-related data from a compliance perspective, and implementing industry-specific data protection requirements. In December 2020, a recommended national standard, the Information Security Technology – Guide for Healthcare Data Security was released to provide comprehensive guidelines in protecting healthcare data, particularly in light of the rapid development of digital healthcare. More healthcare data-related regulations are expected to be issued in the not-too-distant future.

Additionally, in April 2021, the NHSA issued the Guidance on Strengthening Network Security and Data Protection, which requires the establishment of a more solid foundation for network security and data protection mechanisms in digital medical insurance and digital healthcare.

From a general perspective, following two important data protection laws which took effect in 2021, the PRC Personal Information Protection Law and the PRC Data Security Law, a series of measures and guides related to data protection have been promulgated since 2022 regarding detailed regulations on data protection and security assessment measures for cross-border data transfer.

2.3 Regulatory Enforcement

Currently, the key areas of regulatory enforcement in digital healthcare include cybersecurity, personal data protection, and internet-based diagnosis and treatment (including internet hospitals).

In terms of cybersecurity, the implementation of the Multi-Level Protection Scheme (MLPS), which is a compulsory legal obligation under the PRC Cybersecurity Law and relevant regulations, is now becoming an enforcement focus for most industries involving sensitive information, including healthcare.

The MLPS is composed of a series of technical and organisational standards and requirements that need to be fulfilled by all network operators in China. As the development and operation of digital healthcare heavily relies on networks and IT infrastructure, it is critical for digital healthcare providers to enforce and complete the MLPS grading process. Pursuant to the Internet-based Diagnosis Measures and the Internet Hospital Measures, healthcare institutions providing internet-based diagnosis services and internet hospitals shall be graded and protected as Grade III under the MLPS regime. Failure to complete the MLPS would lead to administrative penalties including warnings and fines issued by the Public Security Bureau (PSB).

In terms of personal data protection, relevant data protection authorities such as the Cyberspace Administration of China (CAC), the Ministry for Industry and Information Technology (MIIT) and the PSB have been actively enforcing

personal data protection requirements across industries, including healthcare. Industry supervision authorities such as the NHC and the NHSA are also involved in those enforcement actions on healthcare institutions.

In terms of internet-based diagnosis and treatment (including internet hospitals), as well as the basic Licence of Practice of the Medical Institution, issued by the NHC, medical institutions are also required to have the equipment, facilities, information system, technicians and information security systems that meet Level-3 information security protection, to be assessed by the PSB.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

The Cyberspace Administration of China

The CAC is responsible for the overall planning and co-ordination of network security and relevant supervision and administration. In terms of digital healthcare, the CAC's involvement may include regulating the collection and utilisation of personal information, cross-border transfer of healthcare data, and the cybersecurity review of internet hospitals, etc.

The Public Security Bureau

In terms of cybersecurity, the PSB is mainly responsible for enforcing the MLPS and investigating cybercrimes. With respect to digital healthcare, the PSB's involvement may include:

- record filing for MLPSs completed by healthcare institutions (including internet hospitals);
- conducting inspections related to MLPS on healthcare institutions; and
- investigating crimes related to digital healthcare, such as the infringement of personal data and illegal access to information systems.

Ministry for Industry and Information Technology

The MIIT is responsible for:

- regulating the information technology and communications industry;
- recording filing and approval of Internet Content Providers (ICPs); and
- formulating policies and standards on data security, etc.

In terms of digital healthcare, the MIIT's involvement may include regulating related technology development, such as the development of and security requirements for AI technology. In addition, the MIIT actively leads personal data protection campaigns on mobile applications, including apps used in the healthcare industry.

New healthcare technologies have already prompted co-operation and joint enforcement among various authorities in healthcare and non-healthcare industries, especially related to areas such as IT infrastructure, personal data protection and AI technology.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

Preventative care is not a legal term defined in PRC laws and regulations and can be interpreted broadly. In practice, if a preventative care concerns general healthcare consulting, elder care, nursery, massage, fitness or wellness, without making judgement about diseases or giving tar-

geted recommendations towards specific health issues or conditions, it may not fall within the definition of diagnosis and treatment and will not be subject to special regulation. On the other hand, if a preventative care falls within the area of diagnosis and treatment activities (eg, disease screening or vaccination), it can only be performed by a doctor qualified to practice in a medical institution.

4.2 Increased Preventative Healthcare

National polices have increased the awareness of preventative care. The State Council's Opinions for Implementing the Key Tasks Laid out in the Government Work Report of 2022 indicates that the State Council will adhere to the "prevention first" strategy in the "Healthy China Action" and strengthen health education and health management. The General Office of the CPC Central Committee and the General Office of the State Council's Opinion on Further Improving the Medical and Health Service System issued in March 2023 further stresses the ties between prevention and treatment of diseases, and requires relevant authorities to improve health promotion and preventative healthcare services for pregnant women, infants, students, occupational groups and the elderly. The government policies also focus on improving services, such as elder care, and supporting the revitalisation and development of traditional Chinese medicine (TCM), which will encourage awareness of preventative care.

Social trends also reveal the increased need for preventative care. On the one hand, as a result of the rapid development of the national economy and the expansion of the middle class, more consumers have begun to pursue a better quality of life and are willing to pay for preventative care. On the other hand, the outbreak of COVID-19 and the stress of the ageing population with limited social endowment insurance has also contributed to public health awareness.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Under PRC law, there is no clear separation of personal health data and fitness and wellness information. If certain fitness and wellness information also falls within the scope of personal information, information on human genetic resources (HGR) or healthcare big data, it will be regulated accordingly. The legal considerations can be reviewed in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information** and **11.1 The Utilisation of AI and Machine Learning in Digital Healthcare**.

4.4 Regulatory Developments

Currently, there are no detailed regulations focusing on preventative healthcare. However, national policies have been addressing this topic. For example, the 14th Five-Year Plan for the National Development of Undertakings on the Elderly and for the Elderly Service System stated that "preventative healthcare" for the elderly shall be strengthened, which is the prerequisite for developing elderly care services, combining medical treatment and elderly care. The Guiding Opinions on Promoting the High-Quality Development of Family Doctor Contracting Services issued by the NHC, NHSA, etc in March 2022 requires related regulatory authorities to facilitate the provision of public health services, including preventative healthcare, by family doctors. The Guiding Opinions on Further Promoting the Development of Integrated Medical and Nursing Care issued in July 2022 encourages commercial insurance coverage on preventative health care, health management, rehabilitation and nursing care for the elderly.

4.5 Challenges Created by the Role of Non-healthcare Companies

The healthcare industry is subject to relatively strict regulations in China. When a non-healthcare company enters the market by introducing new technologies and the application of existing technologies to healthcare, it must evaluate:

- whether the device using such technologies will be deemed as a medical device; and
- whether the application of such technologies will be deemed as provision of medical services.

In either case, entrants into the relevant market must first obtain a licence.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

Technology Developments Enabling the Enhanced Use of Connected Devices

Connected devices involve a wide range of technologies, including sensing technology, display technology and wireless communication technology. The development of endurance technology also enables the enhanced use of connected devices.

With the above-mentioned technology, the telemedicine platform can automatically collect various vital signs data, upload the data to the hospital control centre and analyse the data in real time, to provide doctors with an early warning to facilitate the provision of telemedicine services.

5.2 Legal Implications

If a telemedicine platform is aimed at providing health education or caring services rather than medical services, the user may claim for liability against the platform owner.

If a telemedicine platform is registered as a medical device and is used by physicians during their practice, the doctor or the medical institution will be held accountable for malpractice. Also, if the product is proved to be defective, the patient may also claim for product liability against the manufacturer or the seller.

5.3 Cybersecurity and Data Protection

In an on-premises or local computing environment, healthcare institutions need to set up and maintain an IT system with a solid foundation for network security and data protection mechanisms. Taking reference from the Administrative Measures for Cybersecurity of Medical and Health Institutions and a series of policies, guidelines and recommended national standards, the healthcare institutions should:

- install and upgrade anti-virus software;
- detect Trojan viruses;
- monitor the access authority on open ports;
- manage the system; and
- carefully keep a system security diary.

Meanwhile, the healthcare institution should also:

- carry out daily information security monitoring and early warning checks;
- establish security incident reporting and response procedures; and
- formulate emergency response plans.

5.4 Proposed Regulatory Developments

A connected device intended for medical purposes is deemed to be a medical device and is subject to the regulations of the NMPA on medical devices.

Due to the features of a connected device, a series of guiding principles have been formulated to address the cybersecurity and information security issues embedded in such devices. For example, in applying for the registration of the connected device as a medical device, the NMPA will ask the applicant to submit materials to prove its capability on cybersecurity, in accordance with the guiding principles. The NMPA also imposes requirements on the manufacturers to ensure the information security of medical device software – ie, to ensure the confidentiality, completeness and availability of the health data in the software.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Definition and Regulatory Authorities

Under applicable PRC laws and regulations, standalone software as a medical device (SaMD) refers to software which has one or more medical uses, does not require medical device hardware to accomplish the intended use, and runs on a common computing platform. A SaMD can be used in conjunction with multiple medical device products based on a common data interface, such as picture archiving and communication systems (PACS), central monitoring software, or in conjunction with specific medical device products based on a common, dedicated data interface.

As for a software product that uses AI, whether it is administrated as a SaMD depends on its intended use, processing object and core function, among other factors. When a software product processes medical device data and its core function is to handle, measure, model, calculate or analyse such data for medical purposes, the product falls within the scope of a SaMD.

SaMDs, like other medical devices, are regulated by the NMPA and its subordinate branches, including for development, registration, manufacturing, sales, post-market risk management and adverse event reporting, etc.

Classification of a SaMD

Under applicable PRC laws and regulations, medical devices are classified into three classes based on their risks:

- Class I is the lowest risk, for which implementation of customary regulation can ensure their safety and effectiveness;
- Class II is moderate risk and requires strict control to ensure its safety and effectiveness; and
- Class III is high risk and demands special measures to ensure its safety and effectiveness.

For SaMDs, the main factor to be considered when rating the risks is the impact of the SaMD on diagnosis and treatment results. SaMDs having slight impact on diagnosis and treatment results are classified as Class II medical devices, and SaMDs having substantial impact on diagnosis and treatment results are classified as Class III medical devices.

Generally, SaMDs used for image processing, data processing and image file transmission are classified as Class II devices, while most of the

SaMDs used for assisting treatment (eg, formulating a treatment plan) and for assisting diagnosis (eg, giving clinical diagnosis and treatment basis and/or advice) are classified as Class III devices.

Regulations on SaMDs

Registration and updates of SaMDs

Class II medical devices manufactured in China must register with medical product administration on a provincial level. Class II medical devices manufactured outside the PRC and Class III medical devices must register with the NMPA.

Software updates of SaMDs can be divided into major updates and minor updates. Major updates refer to enhancement that affects the intended uses, environment of use or core function of medical devices. Minor updates refer to enhancement that does not affect the safety or effectiveness of medical devices as well as corrective updates.

Major updates are subject to technical review and prior approval from the authorities, while minor updates do not require approval in advance but should be reported in the following registration for post-market change or renewal.

Manufacturing, sale and use of SaMDs

Manufacturing and sales of SaMDs are subject to corresponding licensing requirements, in particular the Appendix for SaMDs of Good Manufacturing Practice for Medical Devices. In addition, the clinical use of certain types of SaMDs may be subject to additional regulations – eg, using AI-assisted diagnostic technology is subject to self-assessment and filing with the relevant health commission, and must meet the specific rules applicable to the clinical use of such technology.

7. Telehealth

7.1 Role of Telehealth in Healthcare

Internet Hospital

Under the Internet Hospital Measures, internet hospitals can be divided into two categories:

- offline healthcare institutions with their associated internet hospitals – eg, an internet hospital of a certain public hospital; and
- independent online hospitals set up with reliance on offline healthcare institutions – eg, an internet hospital set up by internet companies in co-operation with public hospitals.

Under both categories, internet hospitals may provide internet-based diagnosis and treatment to patients, which are limited to the follow-up visits of some common and chronic diseases, and no internet diagnosis and treatment activities shall be carried out for first-time visits.

Under the Internet Hospital Measures, provided that specific requirements are met, physicians can prescribe for patients on internet-based medical services. Specifically, physicians may issue prescriptions online for certain common diseases and chronic diseases diagnosed previously in an offline hospital, and such prescription shall contain the electronic signature of the physician issuing it. After being reviewed and verified by a pharmacist, the healthcare institution or drug supply company may engage an eligible third party to deliver the relevant drugs to the patient.

Family Doctor Contracting Services

Family doctor contracting services are mainly provided by community healthcare institutions. After signing a family doctor service agreement with residents, family doctors provide relevant services according to the requirements of the

agreement, which may include health management services, health consultation services, outpatient services, rehabilitation, smart-aided therapeutics, drug delivery and medication guidance services, etc. The residents can execute service agreements, make appointments, and accept health consultation and follow-up of chronic diseases through online channels such as websites and apps.

Third-Party Information Platform

In addition to internet hospitals and healthcare institutions that provide internet-based medical services, there are third-party information platforms that provide information services in the industry. These platforms establish partnerships with a large number of healthcare institutions or physicians and facilitate the medical consultation services between the physicians and patients.

Cross-Border Telemedicine

Currently, there is no clear restriction on provision of internet-based diagnostic services by healthcare institutions or healthcare professionals located outside China made to patients located in China; though in practice the platform providing such services may be exposed to regulatory risks as physicians and nurses permitted to provide internet-based diagnostic services under the Internet-based Diagnostic Measures shall only be those registered in the national electronic registration system in China.

Consulting services provided online regarding health status or diseases by healthcare professionals to patients, to the extent such services are provided without giving diagnosis or prescriptions, are not internet-based diagnoses regulated by the Internet-based Diagnosis Measures.

7.2 Regulatory Environment

The NHC issued a series of notices and opinions in 2020 to encourage healthcare institutions to leverage telemedicine and release the pressure of offline delivery of healthcare services. Expanding the coverage of telemedicine and establishing a telemedicine collaboration network are also parts of the requirements to further improve the medical and health service system according to the General Office of the CPC Central Committee and the General Office of the State Council's opinions in March 2023. Although there has been a rapid acceleration of telemedicine, some gaps and issues remain to be resolved and clarified from a national policy perspective, such as the expansion of the scope of internet-based diagnosis and treatment, and the application of internet-based diagnosis and treatment on first-time visits.

7.3 Payment and Reimbursement

During COVID-19, the NHSA and the NHC issued further guiding opinions promoting implementation of BMI reimbursement for internet-based diagnosis. In October 2020, the NHSA issued further detailed opinions on the scope of reimbursement and the requirements for application thereof, laying down the regulation framework for the BMI reimbursement of internet-based diagnosis. Under these opinions, qualified offline healthcare institutions providing internet-based diagnosis may apply for an establishing reimbursement arrangement for their internet-based diagnosis services via the BMI agencies. BMI reimbursement for internet-based diagnosis services may cover both medical consultation fees and drugs.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

Typical Application Scenarios of the Internet of Medical Things (IoMT)

Life-cycle monitoring of medical devices

The use of radio frequency identification (RFID), infrared sensors, GPS and other information sensors could help to achieve real-time intelligent identification, tracking, supervision and management of medical devices in order to enhance hospital management.

Intelligent operating rooms

The operating room is a core department of hospital business operation. With the development of the IoMT, intelligent operating rooms can effectively enhance the integration of modern medical technologies and information technologies. Surgeons can obtain and share information through the IoMT, which helps to significantly improve the efficiency of an operating room and allows for more efficient and focused operations.

Wearable health monitoring devices

Wearable health monitoring devices refer to devices using wearable biosensors for collecting data on an individual's movement and physiological parameters for health management purposes. A wearable health monitoring system is an integrated system with non-invasive detection of human physiological information, wireless data transmission and real-time processing functions.

Technological Developments That Drive the Internet of Medical Things

5G networks

The application of 5G networks has greatly facilitated the IoMT. As IoMT devices have different functionalities and data requirements, 5G networks are usually able to support them all.

NB-IoT

The Narrow Band Internet of Things (NB-IoT) network helps the healthcare industry to accelerate the upgrading of its information technology. NB-IoT cellular technology, as a global unified mobile IoT standard, relies on the cellular network to build a network with wide coverage, low power consumption, large links, low cost and high security, and can meet a variety of application scenarios for low-rate services.

Sensors

Sensors are the basic components of various medical devices. The IoMT is an intelligent service system that connects things, people, systems and information resources according to agreed protocols through sensing devices such as RFID tags, wristbands and wearable devices, to process information and react to the physical and virtual world. Currently, the most common applications of IoMT are sensor-based monitoring applications.

Regulatory issues for the IoMT

Currently, regulators in China are still developing the applicable laws and regulations for the IoMT. The main issues under discussion include cybersecurity and personal data protection, especially for handling security risks such as network vulnerabilities. It is critical to timely identify any vulnerabilities and take corresponding remediation measures.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

The Impact of 5G Networks

For digital healthcare development, one of the biggest challenges is the transmission of bulk data, especially for application scenarios such as emergency treatment, where the need for transmission of bulk data in a secured and stable manner is in high demand. A typical scenario is where doctors in an ambulance could use 5G medical devices to complete a series of examinations such as blood tests, electrocardiograms (ECGs) and ultrasounds, and transmit a large amount of data such as images and condition records back to the hospital in real time through the 5G networks, thus substantially enhancing the management of emergency treatment.

In areas such as remote monitoring, remote analysis, remote control and remote diagnosis, where data is collected from various sources in disorder format, 5G networks also help to solve the issues of data sharing and cleaning to support the development and application of AI technologies. In this regard, from 2019 and led by the NHC, several sub-standards of Hospital Network Construction Standards Based on 5G Technology were compiled and released to guide the construction of a new generation of 5G network infrastructure of hospitals.

The Commercial and Contractual Considerations of Healthcare Institutions

Key commercial and contractual considerations faced by healthcare institutions in entering into arrangements with telecommunications providers to deploy and manage 5G networks may include the following:

- whether industry application standards are well developed and applied;
- whether 5G frequency resources are adequately ensured;
- whether 5G application security risk is properly assessed and addressed; and
- whether adequate support for cross-industrial innovation could be supplied.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

Key Legal Issues in Using and Sharing Personal Health Data

Under the PRC data protection framework, general privacy laws and regulations such as the PRC Cybersecurity Law, the PRC Civil Code and the PRC Personal Information Protection Law regulate the protection of personal data and set up the fundamental principles and general requirements, while the healthcare regulation of personal health information provides more specific protection requirements on healthcare data.

Defining personal health data

Under relevant PRC laws, regulations and national standards, personal health data is defined broadly as data that can identify a specific natural person or reflect the physical or mental health of a specific natural person, either alone or in combination with other information. Informed consent is, in principle, the default mechanism for any collection, use and sharing of personal health data, while under special circumstances such as those involving public interest or personal security, consent would not be required.

Broad data requirements

In terms of scientific research and clinical settings, the general requirement of consent would apply for the collection, use and sharing of personal health data unless the data is processed as a "limited data set", which means the data is subject to a certain degree of de-identification but may still identify the specific individual as health data is personalised. The possibility of re-identification is addressed through other technical and organisational protection measures, such as strengthening the internal control process by limiting the data access on a need-to-know basis.

Nevertheless, if de-identification is applied, which facilitates the purpose of preventing the specific individual from being re-identified without additional information, the data would then not be deemed as personal health data, but as general health data, subject to a relatively low level of protection. As for data aggregation, this would not change the nature of personal heath data unless the aggregated data does not contain any personally identifiable information that could be used to identify a specific natural person.

Consent

In terms of consent, digital healthcare has not yet substantially changed the nature of patient consent; instead, it could provide more alternative means for obtaining consent. Informed consent requires a data controller to provide a holistic view regarding the scope and purpose of data collection, use, share, transfer and retention, based on which the data subject could provide a voluntary consent through active conduct. In practice, consent is frequently obtained through:

- clicking on the consent button of a terminal device by a data subject;
- handwritten signatures by a data subject in both electronic and paper format; and
- recording the oral expression of consent made by a data subject.

Legal Considerations in Sharing Personal Health Data

Key legal considerations in sharing personal health data with healthcare institutions or non-healthcare institutions would usually include the following.

- Restriction on sharing – whether there are any restrictions imposed by PRC laws that prohibit sharing of specific categories of personal health data. For example, HGR, including HGR materials and HGR information, are not allowed to be shared with foreign parties without explicit approval or record-filing from the relevant authorities.
- Cross-border data transfer – whether the personal health data would fall within the scope of certain types of data that are required to be stored within the territory of China and are subject to security assessment and approval before being exported to other jurisdictions.
- Informed consent – whether informed consent from the data subject is properly obtained and whether special circumstances under which consent is not required are met.
- Necessity and legitimacy – whether such sharing of personal health data is conducted based on necessity and to achieve legitimate purposes.
- Data security – whether adequate security measures are designed and implemented for the data sharing.
- Due diligence on transferee – whether a proper due diligence process has been completed on the capability of the transferee to ensure data security of the personal health data.

- Contractual agreement – whether a contractual agreement that stipulates the respective rights and obligations (including but not limited to security obligations of the transferee, scope of use by the transferee, restriction on sharing, retention period and disposal requirements, assumption of liabilities for data breach) has been concluded between the transferor and transferee.

Liabilities

As personal health data largely falls within the category of personal sensitive data under PRC laws, the scope of liability for data breach or unauthorised use of or access to personal health data in use and sharing are currently the same as for personal data, and are regulated under the PRC Criminal Law, the PRC Cybersecurity Law, the PRC Civil Code, and the PRC Personal Information Protection Law, which include criminal liabilities, administrative liabilities and civil liabilities as follows:

- criminal liabilities for infringement of personal data include criminal detention, a fixed-term sentence and monetary fines depending on the severity of the conduct and consequences;
- administrative liabilities for illegally processing personal data include written warnings, confiscation of illegal gains, monetary fines (up to RMB50 million or 5% of the turnover of the previous year), suspension of business and revocation of business licences under serious circumstances;
- personal liabilities imposed on the person in charge include fines of up to RMB1 million and prohibition from holding certain positions; and
- civil liabilities for infringement of personal data could be divided into tortious liabilities and liabilities for breach of contract.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

AI, Machine Learning and Data Security Concerns

AI in healthcare is developing rapidly in China and has been playing a robust and growing role in the healthcare industry. Since 2016, with the strong support of national policies, China's giant technology companies have entered into this field and launched different types of AI products. From the legislative perspective, the NMPA issued the Guiding Principles for the Review of Registration of AI Medical Devices in 2022, to regulate the registration of AI products as medical devices. As the most common form of AI, machine learning is widely applied in various aspects such as AI-assisted diagnostics and treatment, medical imaging, precision medicine, pharmaceutical research, followed by data security concerns with respect to the protection of large-scale personal sensitive data and cyber-attacks.

For example, in April 2020, the server of a Chinese healthcare AI company in medical imaging related to COVID-19 diagnostics was hacked, and the research results, source codes and user data were posted on the dark web for sale. The implications of this incident have already exceeded the scope of commercial or business considerations, and from a broader perspective, would even endanger public security and public interests given the involvement of personal sensitive data and important research results for public health.

Likewise, there are strengths and weaknesses of a centralised electronic health record computer system. Strengths include better integration of healthcare resources and more efficient and

effective delivery of healthcare services, while the weaknesses would still include data security concerns, especially when the centralised nature of the electronic health record computer system makes the whole system and data more vulnerable to cyber-incidents or cyber-attacks.

Data Use and Data Sharing in the Machine Learning Context

Similar to other application scenarios, data use and sharing in the machine learning context are subject to the requirements of informed consent and data security under the relevant laws and regulations, such as the PRC Cybersecurity Law, the PRC Civil Code and the PRC Personal Information Protection Law.

Additionally, as a sizeable amount of data from various data sources is required in the machine learning context, the aggregated data may be deemed as healthcare big data and subject to special rules of data localisation, strict electronic real-name authentication and data access control, data classification, important data back-up and data encryption, etc, under the Measures on Healthcare Big Data.

Natural Language Processing

Natural language processing is now widely used in scenarios such as healthcare data mining, converting unstructured healthcare data to structured data, electronic medical records, and medical imaging. As for the regulatory scheme, China is in the process of establishing laws and regulations, ethical norms and policy systems in AI development and application.

11.2 AI and Machine Learning Data Under Privacy Regulations

As addressed in **11.1 The Utilisation of AI and Machine Learning in Digital Healthcare**, companies engaging in new digital healthcare technologies should be aware of the relevant regulatory and legal issues, including cybersecurity and data protection, and that they are subject to the same requirements.

Unlike traditional medical devices, the development of an AI medical device may need a tremendous amount of data for machine learning and training. According to the national recommended standard on Information Security Technology – Guide for Health Data Security, the development and validation phase of a product where data relating to patients and related populations is required is essentially a clinical study. Collecting and processing personal information in a clinical study is also subject to the informed consent of the data subjects. In practice, as the digital companies may not need such data to be identifiable, they may choose to use a "limited data set" subject to a certain degree of de-identification which will not be deemed as personal information.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Licence to Practice

As addressed in **4.5 Challenges Created by the Role of Non-healthcare Companies**, new market players developing new digital healthcare technologies must first decide:

- whether the device will be deemed a medical device under PRC law; and
- whether the application of the device and/or the technologies will be deemed as providing a medical service.

In either case, entrants to the relevant market should first obtain a licence to operate and con-

tinuously follow the regulations of the healthcare industry.

In particular, due to the evolving nature of digital healthcare technology and the need for constant updates, any update of an algorithm due to increased amounts of data may require a change of registration of the medical device, which will need to be submitted to regulatory authorities for re-approval.

Cybersecurity and Data Protection

As addressed in **10. Data Use and Data Sharing** and **11. AI and Machine Learning**, companies engaging in new digital healthcare technologies should pay attention to the legal requirements for cybersecurity and data protection.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

Pursuant to the requirements of the NHC on the construction of information platforms, the IT infrastructure of a healthcare institution should have:

- the core functions of data transmission and data interaction;
- an electronic medical record system; and
- a hospital resource planning system.

Looking forward, a solid foundation for digital healthcare or "Internet Plus Healthcare" could be established through:

- data management and integration of various data resources;
- unification and standardisation of data resources models;
- integration of healthcare services and platforms; and
- elimination of information gaps among departments of the healthcare institution.

This would aim to achieve the goals of:

- resource sharing and business collaboration of healthcare services;
- supply of medical products;
- medical insurance; and
- comprehensive management.

From a cybersecurity and data protection perspective, any IT infrastructure needs to complete the MLPS, which is a compulsory legal obligation under the PRC Cybersecurity Law and relevant regulations. The MLPS includes a series of technical and organisational standards and requirements that need to be fulfilled by the operators of the IT infrastructure.

13.2 Data Management and Regulatory Impact

In 2018, the NHC issued the Standards and Norms for Hospital Information Construction in China (Trial), which provides detailed requirements and standards for various levels of medical institutions with regard to software and hardware construction, security protection and application of emerging technologies, with IT upgrades as one of the requirements.

As for regulations on data management practices, other than the oversight of personal health information, as addressed in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**, patient information and other sensitive data should be stored within the PRC. A medical institution is required to enhance the informatisation level of clinical diagnosis and treatment and the use of electronic medical records, including:

- strengthening the protection of information systems;
- safe storage;
- disaster recovery and back-up of medical data; and
- prevention of information leakage.

14. Intellectual Property

14.1 Scope of Protection

Scope of Protection of Intellectual Property Rights

Technologies involved in digital health technologies or products may be protected by patent right, copyright, or as trade secrets.

Patents

The PRC Patent Law protects inventions, utility models or designs that possess novelty, creativity and practicality. Under the PRC Patent Law:

- an invention means a new technical plan proposed for a product, a process or an improvement thereof;
- a utility model means a practical new technical plan proposed for the shape or structure of a product or a combination thereof; and
- a design means a new design of the whole or part of a shape or pattern of a product or a combination thereof, as well as a combination of colour, shape and/or pattern, which creates an aesthetic feeling and is suitable for industrial application.

There are certain exceptions not protectable by the PRC Patent Law due to a lack of technical features or public interest, including diagnosis and treatment methods for diseases, rules and methods of intellectual activities, etc. AI technology can be protected as a patent to the extent such technology meets the requirements, for which purpose it should not only be in the form of algorithms, but also have certain technical features. The terms of protection, commencing from the application date, are:

- 20 years for inventions;
- 10 years for utility models; and
- 15 years for designs.

Copyright

The PRC Copyright Law protects works in the fields of literature, art and science which can be expressed in a certain form, including, without limitation, written works, oral works, photographic works, audio-visual works, graphic works and model works (such as engineering design plans, product design plans, maps and schematic diagrams), computer software, etc. Therefore, with respect to technologies and products in the field of digital health, computer software and product designs, among others, can be protected by copyright.

The duration of a copyright depends on the type of author and type of such work – ie, the protection term of right of authorship, right of revision and right to preserve the integrity of the work of an author is eternal, whereas the protection term for the right to publish the works of an entity is 50 years from the completion of the works.

Trade Secrets

Under PRC laws, trade secrets refer to commercial information such as technical information and business operation information not known to the public, that has commercial value and for which the rights holder has adopted the corresponding confidentiality measures. Non-public information related to AI technologies, such as certain know-how, can be protected as a trade secret, provided the appropriate confidentiality measures are adopted.

Protection of Data

If data is expressed and exhibits originality, hence constituting a work, such data may be protected by copyright. Data can also be protected as a trade secret in China. With respect to a database, if the selection or compilation of its content shows originality, it may be protected as a compilation work under the PRC Copyright Law. In addition, if utilisation of the data or database obstructs the competition order of the market and constitutes unfair competition, the PRC Anti-unfair Competition Law may also apply.

AI Inventorship and Authorship

Whether AI can be regarded as an inventor of invention developed by AI has not yet been clarified under the PRC Patent Law. Currently, work generated with the assistance of AI (ie, an article written by AI but with the input of data, template and writing style determined by the employees of a company) is eligible for copyright protection with such work deemed work-for-hire and with the company regarded as the author.

14.2 Advantages and Disadvantages of Protections

To decide which form of intellectual property protection applies to certain technology, the characteristics of the technology – ie, whether it satisfies the requisite elements of a specific form of intellectual property – need to be considered.

If the technology satisfies the features of more than one form of intellectual property, commonly between a patent and a trade secret, the technology owner needs to be aware of the advantages and disadvantages of different types of protection.

A patent right can be better claimed, proved and valued as it is reviewed and granted by the Patent Office and officially registered. Such protection is granted on the condition that the technology is reviewed, publicised and the protection duration is limited under the law.

Trade secret protections, on the other hand, require the owner to take relevant measures to keep such technology confidential and the protection does not have a time limit as long as the technology remains unknown to the public. However, in the case of a trade secret infringement, the owner will have to prove the existence of the trade secret, their rightful ownership, the occurrence of the infringement and its value.

14.3 Licensing Structures

The licensing arrangement of intellectual property could be different, depending on the commercial needs.

Provision of Services or Sale of Products

The provision of services or sale of products will not include a proprietary transfer of the intellectual property embedded in the services or products to the purchaser of the services or products. Similarly, the purchasers are not automatically granted a licence regarding the intellectual property except for the use of services or products they purchased for their intended use.

Licence Deal on Digital Healthcare Products or Technology

In a typical licence deal, the licensor will grant a licence to the licensee to develop, utilise, upgrade, improve and commercialise the digital healthcare products or technology. Such collaboration will generally include a licence of intellectual property rights and the consideration for such a licence, under which the licensee can use the intellectual property for agreed purposes and retain interest generated therefrom. Sometimes, the licensor will also ask for a right of grant-back to enjoy the improved technology and a right of

reference of the data generated from the licensee's use of the licensed products or technology.

Co-development

For digital healthcare services and products that are at an early stage of development, the parties may agree on a co-development of such technology or product and co-own the intellectual property rights derived therefrom.

14.4 Research in Academic Institutions

Copyright Allocation

With respect to works created by a physician employed by a hospital or a researcher employed by a university while performing their work, unless otherwise agreed, the copyright of the work shall be owned by the physician or researcher, provided that the hospital or university as employer shall be entitled to use such work within the scope of its operation. However, for works created primarily using material and tools of the employer – ie, the hospital or the university – the copyright shall be owned by the hospital or the university (except that the right of authorship belongs to the employee) unless otherwise agreed.

The copyright of a work jointly created by two or more persons shall be co-owned by the co-authors. Attribution of copyright of a commissioned work shall be agreed between the principal and the commissioned party via a contractual arrangement. Where the contract is not clear or where there is no contract, the copyright shall belong to the commissioned party.

Patent Right Allocation

If an invention is developed by a physician employed by a hospital or a researcher employed by a university while performing their work or mainly utilising materials and tools of the hospital or university, the patent right of such invention belongs to the hospital or the university unless otherwise agreed between the parties.

Where two or more entities or individuals co-operate in the development of an invention, or if an entity or individual has been engaged by another entity or individual to develop an invention, unless otherwise agreed, the entities or individuals that have completed or jointly completed the invention shall own or co-own the patent application right and patent right (if granted).

It should be noted that, with respect to patent applications for work products generated from international co-operative research (eg, between a Chinese hospital and a foreign sponsor) utilising Chinese HGR, at least as regards clinical trials for non-registration purposes, such patent application should be submitted and the patent rights owned by both parties of the co-operation.

14.5 Contracts and Collaborative Developments

Where multiple parties are involved in the creation of a work or in the development of technologies, subject to applicable laws and regulations, the parties should clearly agree on the ownership of the intellectual property rights of the relevant work product and, to the extent necessary, make detailed and clear arrangements on the exercise of the rights and restrictions thereon, such as rights and restrictions on use, licensing, transfer and profit distribution. Specifically, in clinical trial agreements involving international co-operative research utilising Chinese HGR, appropriate IP provisions must be included to comply with applicable regulations and protect the legitimate interest of the parties involved.

15. Liability

15.1 Patient Care

Generally, with respect to the determination of liabilities in the event injury is incurred by a patient using a SaMD, provisions on product liability and tort would apply – ie, the patient can claim compensation from either the manufacturer or the seller if the injury is caused by a defect in the product. Where the party compensating the patient (either the manufacturer or the seller) is not liable for the defect, such party may recover its losses from the other.

If the defective SaMD was being used by a healthcare institution, including a SaMD using AI technology (to the extent the AI technology is not providing a diagnosis and treatment solely on its own), the patient may also elect to claim for compensation from the healthcare institution, which itself may seek to recover its losses from the manufacturer liable for the defect.

If the healthcare institution is at fault when conducting diagnosis and treatment activities, it shall also be held liable. The question of whether AI can conduct medical treatment independently and the related liability issues are to be further clarified by relevant laws and regulations.

In terms of the potential bias issue of AI, as bias would likely be deemed an ethical issue, this is to be further clarified by enforcement practice.

15.2 Commercial

Contractually, if the supply chain disruption or the cause thereof constitutes a breach of the agreement between the vendor and the healthcare institution, such as a failure of the vendor to perform certain obligations, the vendor shall bear contractual liabilities as agreed by the parties. If such failure constitutes violation of applicable laws and regulations, the vendor may also be subject to punishment by the relevant authorities.

Trends and Developments

Contributed by:
Linda He and Zoe Zhang
Han Yi Law Offices

Han Yi Law Offices is one of the most active and knowledgeable resources in the PRC private equity investment community, and is a leading Shanghai-based Chinese boutique law firm specialised in formation and deployment of private equity and venture capital funds, M&A, securities, banking and finance, and foreign related dispute resolutions. With around 20 lawyers, Han Yi Law Offices regularly represents world-class private equity investors, venture capitalists, active industrial investors, hedge funds and PRC state-owned investment arms targeting essentially all major industry areas in a wide variety of private equity transactions, including buyouts (leveraged and non-leveraged), early and late-stage venture investments, restructurings, going private and recapitalisations, and exit transactions. The firm has a proven track record of structuring and executing innovative and complex cross-border private equity and venture capital investment deals and M&A transactions involving buyouts, follow-on acquisitions, IPOs, and trade sales, among others.

Authors

Linda He is the managing partner of Han Yi Law Offices, experienced in private equity and venture capital investments, M&A, restructurings, financing, and various Chinese regulatory compliance matters. Ms He is the routine counsel to several leading international private equity investors and some of the most active PRC fund managers on their Chinese investment deals. She is well known for her deal structuring talents and her fast and reliable deal execution abilities, especially for complex cross-border transactions involving multiple parties. She is particularly experienced with private equity and venture capital deals involving such industries as healthcare and life sciences, financial services, education, logistics and lodging.

Zoe Zhang is a counsel of Han Yi Law Offices. She specialises in the areas of M&A and private equity investments, regulatory compliance, dispute resolution and general corporate matters. In the private equity and M&A areas, Ms Zhang has been actively involved in advising numerous reputable private equity and venture capital funds, including their portfolio companies, from a variety of industries such as healthcare, pharmaceuticals, e-commerce, TMT, and leisure and tourism. Before joining Han Yi Law Offices, Ms Zhang was an in-house counsel with a well-known foreign-invested company in China, where she was involved in various regulatory compliance matters and in commercial dispute resolution.

Han Yi Law Offices

Suite 1801,
Tower I,
Huayi Plaza
2020 West Zhongshan Road
Shanghai 200235
China

Tel: +86 21 6083 9800
Email: inquiry@hanyilaw.com
Web: www.hanyilaw.com

Overview

Digital healthcare is not yet a clearly defined term under the current People's Republic of China (PRC) legislative framework. In practice, digital healthcare in China is generally referred to as "the application of digital technologies in the medical and health sectors", which mainly includes internet hospitals, online pharmacies, AI-based medical devices, big data and medical robots, among others. The rapid growth of emerging technologies and the continuous support from the Chinese government has caused a digital transformation and the acceleration of China's healthcare sector in recent years. This in turn has improved the quality and efficiency of healthcare services and hospital management.

The outbreak of the COVID-19 pandemic in early 2020 drove wider acceptance of telemedicine and forced online platforms to provide a full range of services covering online diagnosis and treatment, drug sale and delivery, and online payment, as well as medical insurance reimbursement services. By the end of 2022, the Chinese government had approved a total number of 2,700 internet hospitals, with the number of users of internet-based medical services in China reaching 363 million. The market size of internet hospitals and online pharmacies reached around RMB310 billion and RMB250 billion respectively, representing an increase of approximately 39% and 36% correspondingly, on a year-on-year basis. However, it remains unclear whether the demand for internet hospitals and online pharmacies boosted by the COVID-19 pandemic will continue to rise in the post-COVID-19 era.

The boom of investments in China's digital healthcare industry in 2021 was subsequently followed by a slowdown in 2022 along with the economy's downturn in general. According to statistics, the total financing amount in the main sectors of China's digital healthcare industry (eg, internet hospitals and online pharmacies) in 2022 was approximately RMB4 billion, down by over 80% on a year-on-year basis, while the total number of financing transactions declined by around 40%.

New Technologies and Applications

With advances in digital technologies such as the internet, AI, robotics, 5G, blockchain, big data and 3D printing, China's healthcare sector is entering an era of full digitalisation by applying new technologies in various healthcare service scenarios, including disease prevention, diagnosis, surgery, hospital management, health management, healthcare data analysis and processing. The following are the main applications

of these new technologies in China's healthcare sector.

Telemedicine or online healthcare

Telemedicine has become one of the most popular and fast-developing areas of China's digital healthcare industry, as a result of the innovative applications of internet technology and the implementation of national policies promoting "Internet Plus Healthcare".

From the regulatory perspective, telemedicine services can be generally divided into the following two categories.

- Online diagnosis and treatment services – which under applicable laws and regulations are generally limited to online diagnosis, treatment and prescription services for subsequent visits of outpatients. Providers of internet-based diagnosis and treatment services are required to be licensed medical institutions (also known as internet hospitals) in addition to meeting the qualifications necessary for the operation of internet platforms.
- Non-diagnosis healthcare services – which mainly include non-diagnosis medical and health consultation, online hospital appointment registration, drug sales and delivery. Operators providing these online services do not have to be licensed medical institutions, while other qualifications for the operation of internet platforms may still be required.

The establishment and operating models of internet hospitals are becoming more diverse. In the early stages, internet hospitals were mainly sponsored by large internet providers together with certain private hospitals. Driven by the COVID-19 pandemic, many public hospitals launched their internet hospitals to extend their medical services. Other players in the healthcare system, such as insurance companies and pharmaceutical companies, have also participated in the investment and operation of internet hospitals. Meanwhile, the acceleration of reimbursement of internet medical costs by China's medical insurance fund since 2021 has further boosted the internet healthcare industry.

However, despite the fact that large internet healthcare platforms saw a significant rise in their revenues in 2021 and 2022 (especially revenue from the online sale of drugs), their profitability remains relatively low compared to offline services, as the unit price of online services and consumers' willingness to pay for them are also still relatively low and the homogeneity competition in this sector has become quite severe.

AI-based applications

AI technology is one of the core technologies fuelling the expansion of the digital healthcare market, and is being used in a number of areas including disease prediction, clinical decision support systems (CDSSs), drug development and health management, with a prominent area being imaging auxiliary diagnosis. In 2022, the Ministry of Science and Technology (MOST) issued several polices to promote the application and innovation of AI technology in the healthcare industry.

Whether an AI-based medical software or system should be regulated as a medical device under PRC laws mainly depends on its intended functions and usages (see AI-based medical devices for more details). It is worth noting that, since the National Medical Products Administration (NMPA) approved the first Class III AI-based medical device in early 2020, the commercialisation and approval process of these devices has gradually accelerated. In 2022, the number of approved AI medical software reached a record

high with a total of 25 Class III medical device licences issued by the NMPA.

With the advent of more advanced applications of AI technology (eg, the launch of ChatGPT) in 2022, development of AI-doctor products providing diagnosis and treatment services has captured the market's attention. It is reported that some online healthcare companies in China will soon launch their first AI-doctor products in the market. As China's existing regulations specifically prohibited AI from replacing physicians to provide diagnosis and treatment services, the legal basis and framework for the commercialisation of AI-doctor products is still pending further clarification from China's authorities.

Medical robots

The use of medical robots in China has been growing rapidly since 2019, and they have been applied in various healthcare scenarios (eg, medical guidance, surgery, rehabilitation and nursing) to enhance efficiency and accuracy in healthcare services. However, China's medical robot market is still in its early stage compared to the United States and Europe, mainly due to its high cost and safety concerns. With the aim of boosting application and funding of medical robots, China issued a series of supportive policies in 2021–2022 in this sector, benefiting medical robot market players and consumers.

According to statistics, in 2022 the NMPA approved over 15 domestic surgical robots, twice the number of those approved in 2021; and the market size of China's surgical robots is expected to reach RMB12 billion by 2023.

Smart hospitals and 5G

With the aim of optimising medical services and streamlining diagnosis and treatment, China released a series of supporting policies for building smart hospitals in 2022, which are based on the implementation of electronic medical records (EMRs) systems and other information systems. The application of smart hospital solutions has gradually become a key performance assessment and evaluation indicator for public hospitals in China.

5G technology plays a crucial role in the construction of smart hospitals, especially in the area of remote teleconsultation, by allowing access to patients' records in seconds, sharing medical images and obtaining virtual guidance from experts in different fields in real-time. In September 2021, China's Ministry of Industry and Information Technology (MIIT) and the National Health Commission (NHC) announced the "5G+ Medical Health" pilot projects, which are aimed at fostering innovative products and business models in the 5G medical healthcare industry. It is expected that 5G network coverage will become one of the main goals for hospital infrastructure upgrades.

Healthcare data and blockchain

Healthcare data mainly refers to data generated in the process of disease prevention, medical treatment and health management. The tamper-proof feature of blockchain technology could help to build up a system featuring credible storage, compliance data sharing and whole-process traceability of healthcare data. In recent years, the NHC and its local counterparts have been making efforts to set up a nationwide healthcare data infrastructure (eg, an all-citizen health information platform and medical health big data centre) by using big data and blockchain technologies with the intention to facilitate interconnectivity and information sharing between hospitals.

In May 2022, a national unified medical insurance information platform was established, with an effort to facilitate information sharing between social insurance authorities and medical institutions at all levels across the country. It is expected that all public medical and health institutions in China will get connected to this national health information platform by 2025.

3D printing

As an important and frontier area in the application of 3D printing technology (also known as additive manufacturing technology), medical 3D printing has been used by hospitals in China mainly in pre-operative planning, surgical guides and patient-tailored implants. Though medical 3D printing has significantly improved the personalisation and accuracy of medical services, currently its application in China is relatively limited and mainly focuses on external medical devices for dental and orthopaedic applications.

The MIIT issued a strategic plan in 2021 to propose the development of new products in the field of "3D printing plus medical health" and the promotion of customised medical services and devices such as rehabilitation equipment, implants and soft tissue repairing treatment. Some provincial governments have gone further and have set up pricing guidance and policies for medical 3D printing devices in an effort to ensure costs related to medical 3D printing are covered by local medical insurance and are more affordable for patients.

Digital therapeutics

Digital therapeutics (DTx) is a relatively new concept in the digital healthcare industry, and generally refers to evidence-based medical interventions driven by software programs for disease prevention, management and health improvement. As DTx products may also apply AI technology, there could be an overlap between DTx products and AI-based medical devices.

DTx has attracted market attention in China in recent years, with an increasing number of DTx products obtaining medical device licences and being launched in the market. It is noteworthy, however, that the definition, classification and technical criteria of DTx remain unclear under China's existing regulatory framework. To duly address these issues, the NMPA was reported to have organised a meeting with experts to discuss and study the DTx field at the end of 2022; and regulatory guidelines for the DTx sector are expected to be released in due time.

Major Regulatory Developments in the Digital Healthcare Sector

The legislative and regulatory developments in China's digital healthcare sector since 2021 have mainly focused on the following areas.

Foreign investment

The Chinese government has continued its efforts to further open the digital healthcare sector to foreign investors in recent years. Following the release of local policies to encourage eligible foreign investments in "Internet Plus Healthcare" by the Beijing Municipal Commerce Bureau in December 2021, the State Council released the *Revisions to Administrative Provisions on Foreign-Invested Telecommunications Enterprises* in April 2022. This regulation is expected to further facilitate foreign investment in the digital healthcare sector by substantially relaxing qualification requirements for such investors in online healthcare platforms that hold the Value-added Telecommunications Business Licence.

However, with respect to businesses involving collection, storage, provision or otherwise processing of personal information, human genetic

resources, sensitive healthcare information, or information having national security concerns, the Chinese government has tightened its regulations on foreign participation (see Healthcare data protection for more details).

Telemedicine and online healthcare

China launched three regulations in 2018 (the *Administrative Measures for Internet-based Diagnosis and Treatment* the *Administrative Measures for Internet Hospitals* and the *Good Practices for Telemedicine Services* all for Trial Implementation) to provide a general legal basis for the administration of telemedicine and other online healthcare services. With the rapid development of China's internet healthcare industry, a variety of non-compliant practices and malpractice phenomena in the Chinese internet healthcare industry also sprang up, including:

- online malpractice by disqualified physicians;
- online diagnosis by AI rather than by qualified physicians;
- lack of standard operating procedures and guidelines for online diagnosis and treatment;
- prescription of drugs which could not be prescribed online; and
- operation of online diagnosis and treatment platforms by unqualified operators.

With an aim to address these issues, the NHC officially released the *Detailed Rules for Regulation of Internet-based Diagnosis and Treatment (Trial)* in June 2022, putting forward detailed requirements for operators of internet diagnosis and treatment platforms, their personnel, business scope, service quality and safety, among others. To reinforce the supervision on safety and quality of online medical services, the rules specified that, to the greatest possible extent, the internet-based diagnosis and treatment services provided should be of the same quality as those provided by medical institutions offline.

It is also worth noting that the *Circular on Boosting the Provision of Internet-based Medical Services for COVID-19* issued by the NHC in December 2022 conditionally allowed internet hospitals to provide first-time diagnosis and treatment of COVID-19-related symptoms. The market generally expects that first-time diagnosis and treatment of more types of common and chronic diseases may be available online in the future.

Furthermore, the National Healthcare Security Administration and the NHC have released a series of supportive policies in terms of pricing management of and medical insurance reimbursement for "Internet Plus Healthcare" services. The National Development Reform Commission also issued an implementation plan in December 2022, further clarifying that certain internet medical services will be included in the scope of China's medical insurance payment system. Currently, most governments at the provincial level have issued local pricing policies and guidance for "Internet Plus Healthcare" services. It is believed that these regulatory efforts and favourable policies will facilitate the rapid advancement of China's internet healthcare industry.

AI-based medical devices

In 2017, the NMPA updated the *Catalogue of Medical Device Classification* to formally classify AI-based medical software (including analysis and processing software for medical imaging and pathology images, decision-supporting software, treatment planning software, rehabilitation training software, etc) as Class II or Class III medical devices for the first time. With the ever-changing development and innovative

adoption of AI technologies in medical software, it is still difficult to determine whether a novel application of AI medical software should be regulated as a medical device and which category of medical device it falls into, according to the classification criteria under the existing rules. This has brought compliance uncertainties and confusion to many developers and manufacturers of AI-based medical devices.

In order to establish a clearer regulatory direction for medical AI applications, the NMPA issued the *Guidelines for Classification and Definition of Artificial Intelligence Medical Software Products* in July 2021, which defined AI medical software as AI-powered software to be used for medical purposes by processing data from medical devices. The Guidelines also elaborated on key factors to consider when determining the classification of AI medical devices, including the intended use of the product (eg, whether it is for supporting a physician's decision-making) and its algorithm maturity. In March 2022, the NMPA released three guidelines further streamlining and optimising China's review and approval system for AI-based medical devices:

- the *Registration and Review Guidelines for Artificial Intelligence Medical Devices*;
- the *Registration and Review Guidelines for Medical Device Software*; and
- the *Registration and Review Guidelines for Medical Device Cybersecurity*.

In addition, the NMPA successively released several guidelines in 2022 to further specify the requirements for registering certain typical AI medical software products.

Healthcare data protection

In the absence of unified and specific legislation on data protection in the healthcare sector in China, regulatory requirements on healthcare data protection are scattered throughout various general laws and regulations, as well as throughout national standards and industry guidance. A series of new regulations and policies have been announced by the Chinese government since 2021, in an effort to strengthen data protection and online security in the healthcare sector, which include the following.

- The *Personal Information Protection Law* issued in August 2021 classified personal information on medical health as "sensitive personal information" which should be afforded a higher level of protection than ordinary personal information.
- The *Data Security Law* and the *Administrative Regulations on Network Data Security (Draft for Comments)* issued in June and November 2021 respectively, proposing to establish a data classification and graded protection scheme, through classifying data as "important data", "core data", and "general data" and requiring corresponding protection measures to be taken for different categories of data. It is noteworthy that genetic and other healthcare data that meet a certain scale or accuracy level (eg, data concerning more than one million pieces of personal information) as required by relevant authorities are classified as "important data" (detailed catalogues of "important data" are yet to be formulated) and thus will subject the data processors to some special protection requirements for "important data".
- The *Measures for Network Security Review and the Measures for Security Assessment of Outbound Data Transfers* released in December 2021 and July 2022, respectively, further required that healthcare data processors must apply for a government-led security

review or assessment in any of the following circumstances:

(a) outbound transfer of "important data" by a data processor;
(b) outbound transfer of personal information by a Critical Information Infrastructure Operator (CIIO; the guidance on identifying such operators remains to be further clarified) or a data processor who has handled more than one million pieces of personal information;
(c) outbound transfer of personal information by a data processor who has provided personal information of 100,000 people abroad cumulatively or sensitive personal information of 10,000 people abroad cumulatively in the previous year;
(d) listing abroad by a healthcare data processor who has handled more than one million pieces of personal information; and
(e) any other data processing activity which has or may have national security concerns.

- The *Detailed Rules for Regulation of Internet-based Diagnosis and Treatment (Trial)* released in June 2022 required that platforms providing online diagnosis and treatment services should go through registration or filing procedures applicable for the third level of information security protection systems. They should also establish internal mechanisms and enter agreements with relevant partners in relation to cybersecurity, personal information protection and data use management.
- The *Administrative Measures for Cybersecurity of Medical and Healthcare Institutions* issued in August 2022 further detailed the network and data security protection obligations of medical institutions as network operators, CIIOs and data processors, providing more practical guidelines for medical institutions in terms of compliance with existing regulations on network and data security.
- The MOST published the *Implementing Rules of Administrative Regulations on Human Genetic Resources Management* in June 2023, which beefed up regulations on collection, preservation, utilisation and provision of human genetic resources derived from China ("China HGR") for non-clinical purposes, especially prohibiting foreign entities or individuals from collecting or preserving China HGR or providing China HGR abroad.

Prospects and Challenges

With the continuous and strong support from the Chinese government and the accelerated adoption of emerging technologies in various healthcare sectors, China's digital healthcare industry has entered a golden period of development. It is expected that the Chinese government will maintain its supportive policies for the digital healthcare industry in the coming years, and consumers' demand for intelligent, personalised and efficient healthcare services will continue to rise. According to statistics, the market size of China's digital healthcare industry is expected to exceed RMB1.5 trillion by 2025.

Despite the promising future of China's digital healthcare, however, the following major issues and challenges with the business models and legal frameworks remain to be improved.

Data protection

The various types and enormous amount of data generated in the digitalisation of the healthcare sector (including EMRs, clinical trial data, health information, human genetic resources, healthcare big data, etc) are sensitive and valuable resources that will be subject to the supervision of various governmental authorities, posing a challenge to the co-ordination of multiple

supervisors, and requiring clearer guidelines in this regard.

Furthermore, healthcare data leakage and infringements are not uncommon in practice, mainly due to the absence of a specific, comprehensive and operable legal framework for healthcare data protection. Thus, it remains difficult for individuals to pursue appropriate remedies and compensation through effective legal proceedings.

Market access

Laws and regulations do not always keep up with innovative applications of new technologies in the healthcare sector. Consequently, relevant market players usually have to keep in close communication with regulatory authorities on a case-by-case basis in order to realise the commercialisation of novel products and services, as well as reduce compliance risks.

Liability

The existing liability framework may not be able to provide suitable and effective remedies for infringements related to novel digital healthcare services and products. For example, if medical accidents occur when using AI diagnostic tools or surgical robots, the determination and allocation of liabilities among developers, manufacturers and physicians is still a practical challenge.

Payment methods

Currently, only costs related to limited digital healthcare services are covered by medical insurance funds, and the roadblocks regarding expansion to reimbursement by medical insurance funds remain to be lifted.

ECUADOR

Law and Practice

Contributed by:
Jose Meythaler and Karina Loza
Meythaler & Zambrano

Contents

Meythaler & Zambrano is one of the most prestigious law firms in the Ecuadorian market. Founded in 1995, the firm specialises in national and international legal counselling and litigation for international and domestic corporations. The firm´s highly qualified team focuses on regulatory counsel (the pharmaceutical, medical, food, and cosmetic sectors), intellectual property, competition and antitrust, arbitration and mediation, corporate and commercial affairs, dispute resolution, taxes, public procurement, and public law. The firm has offices in Quito and Guayaquil. These offices work throughout Ecuador and belong to a wide network of correspondents throughout America, Europe, and Asia. The firm is a member of the International Bar Association (IBA), the International Trademark Association (INTA), the Intellectual Property Association (ASIPI), and the Ecuadorian Associations of Mediation and Taxation Law.

Authors

Jose Meythaler is the president and main partner of Meythaler & Zambrano. He has advised several companies in public law, corporate law, intellectual property, competition law, investment arbitration, oil law, banking, and pharmaceutical law. As a result of his successful career, he is recommended by several legal publications. He is a referee of the Mediation and Arbitration Centre of the Ecuadorian American Chamber of Commerce and has been president of the Intellectual Property Committee of the Ecuadorian American Chamber of Commerce since 2010. Jose has a Juris Doctorate Degree and is a lawyer of the Courts of the Republic, and has a Bachelor's degree in Juridical Sciences from the Pontificia Universidad Católica del Ecuador.

Karina Loza is a partner of Meythaler & Zambrano. She provides legal advice to different sectors of the industry, including pharmaceutical, agrochemical, cosmetics, food and beverages. She has significant experience in advising on the defence of new technologies, test data protection and illicit market control. She also has extensive experience regarding authorisations, and sponsorship in all types of administrative procedures with the public health and agricultural sectors. She has been a panellist and speaker at several forums on pharmacovigilance, sanitary and phytosanitary legislation, illicit market control, and drug pricing and review.

Meythaler & Zambrano

Av. 6 de Diciembre 2816 y Paul Rivet
Edificio Josueth Gonzalez
Piso 10
Quito
Ecuador

Tel: +593 2 223 2720
Email: info@lmzabogados.com
Web: www.meythalerzambranoabogados.com

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

The Right to Privacy in Ecuador

Personal and family privacy are among the freedoms/rights recognised and guaranteed by the Constitution of the Republic of Ecuador.

The confidentiality of personal information includes ideology, political affiliation, union affiliation, ethnicity, health status, sexual orientation, religion, immigration status and other information related to personal privacy, especially any information whose public use violates the human rights enshrined in the Constitution and any other international instruments.

Any information that has been declared private by the competent authority is also confidential, as well as any information protected under banking or stock exchange secrecy, and any information that could affect the internal or external security of the State.

Health Data

Regarding health information, any technological platforms that collect and store patients' clinical information must have the prior and express consent of the owner of the data.

On 26 May 2021, the Personal Data Protection Law was published, which imposes new rules regarding health information collected to provide health services.

This regulation defines health-related data as personal data relating to the physical or mental health of an individual, including the provision of healthcare services, which reveal information about his or her health status.

According to this law, the treatment of health-related data from a patient must comply with the following minimum parameters, from both a regulatory and a technological point of view.

- The institutions that are a part of the National Health System and any health professionals may collect and process data relating to the health of their patients who are or have been under treatment by them.
- Those responsible for and in charge of data processing, as well as all persons involved in any phase thereof, are subject to confidentiality, and they must ensure adequate security of personal data, including protection against

unlawful processing of this data, and accidental loss, destruction, or damage, through the application of appropriate technical and measures.
- Additionally, health-related data generated in public or private health establishments must be treated in compliance with the principles of professional secrecy. The owner of the data must give prior consent, except in cases where (i) the processing is necessary to protect the vital interests of the owner of the data; (ii) the owner of the data is physically or legally incapable of giving his or her consent; or (iii) this is necessary for preventive or occupational medicine, the assessment of a worker's capacity to work, medical diagnosis, the provision of health or social care or treatment, or the management of health and social care systems and services, based on the specialised legislation on the subject or under a contract with a healthcare professional. In the latter case, the treatment may only be carried out by or under the responsibility of a professional who is subject to the obligation of professional secrecy, by the specialised legislation on the matter or with any other rules that may be established by the Authority in this respect.
- The health-related data to be processed, whenever possible, must be previously anonymised or pseudonymised, avoiding the possibility of identifying the owners of the data.
- Any processing of anonymised health data must be previously authorised by the Personal Data Protection Authority. To obtain the aforementioned authorisation, the interested party must submit a technical protocol containing the necessary parameters that guarantee the protection of that data and the prior favourable report issued by the Health Authority.

1.2 Regulatory Definition

According to Ecuadorian regulations, telemedicine or digital medicine is a mechanism implemented to improve access to health and medical care for people, and link information and communication technology with medicine.

In this way, telemedicine has been regulated in different legal and regulatory instruments, such as Ministerial Agreement No 5169, through which the Operational Guidelines for the Implementation of a Comprehensive Healthcare Model (MAIS) and the Comprehensive Public Health Network (RPIS) were issued in 2015.

However, to date, Ecuador has not implemented a specific regulation on telemedicine that comprehensively develops the management and procedures for the provision of this service; therefore, telemedicine is governed by general rules that allow its application in both the public and private sectors.

The Ministry of Public Health, as the National Health Authority, sought to implement structural changes in the health sector which would serve as a guide for the implementation of the MAIS with a family, community, and intercultural approach, governing the development of the RPIS and the complementarity with the private sector of the National Health System.

Therefore, there are general concepts contemplated in Ministerial Agreement No 5169, which explains, in general terms, certain concepts and procedures for the provision of remote medical health services (telemedicine), which are of direct application, including the following:

- telemedicine – this is defined as the provision of medical health services at a distance, using

information and communication technologies for its implementation;
- telemedicine medical care – this is a system for the provision of health services at a distance, using information and communication technologies for its implementation;
- telemedicine referral is the sending of information from users or elements of diagnostic assistance by electronic means to the operative health units, to other health institutions for medical care or diagnostic complementation;
- counter-referral in telemedicine is the response that the health units receiving the telemedicine referral give to the health body, or the family unit. This response may be as a counter-referral (indications) or with information on the care received by the user in the receiving institution.

On 27 July 2022, Ministerial Agreement 22 was issued by the Ministry of Telecommunications and Information. This agreement includes Digital Healthcare as Pillar 4, with the objective of promoting programmes and projects in digital healthcare, considering the promotion of telemedicine and preventive healthcare services in rural areas and among priority groups.

1.3 New Technologies

Telemedicine, by its nature, is strictly linked to information and communication technologies, replacing, in many cases, the traditional way in which medicine has been provided. Therefore, the provision of remote medical services involves many different services and technologies, including communications, databases, internet and intranet resources, and the transmission and/or filing of images that go beyond the traditional concept of medicine.

In this sense, it is important to consider that Ministerial Agreement 22, issued by the Ministry of Telecommunications, included the Digital Transformation Agenda, which aims to establish a co-ordinated multisectoral work framework that establishes lines of action for the country's digital transformation process, defining its governance and institutional framework, and considering the transversality of information and communication technologies.

Telemedicine is approached for the purposes of the digital transformation agenda as a healthcare service, in which distance is a critical factor, performed by professionals using information and communication technologies to exchange data, make diagnoses, recommend treatments, prevent diseases and injuries, as well as for the ongoing training of healthcare professionals, and in research and evaluation activities, with the aim of improving the health of individuals and the communities in which they live.

Unfortunately, there have been no regulatory advances in this area on the part of the healthcare authorities. This is why the implementation of regulatory frameworks that allow the inclusion of telemedicine platforms for the benefit of patients continues to be a challenge for both the National Healthcare System and telecommunications, but there are no private regulations or limitations.

In this respect, Ministerial Agreement No 016-2018 emphasises the value of promoting telemedicine through pilot projects: "This project aims to help the National Health System (SNS) reach the entire Ecuadorian population, universally and at no cost, through strategic alliances between the public and private sectors, with the application of information and communication technologies, through the Infocentros Project,

thus promoting the development of the information and knowledge society. Implementing a telemedicine/teleconsultation system among the medical staff of the Ministry of Public Health in rural areas, for a second opinion, with the support of specialists of the Medical Systems of the Universidad San Francisco de Quito, through the Infocentros Network, for the benefit of the most vulnerable."

1.4 Emerging Legal Issues

Digital medicine in Ecuador has not been regulated; however, the onset of the COVID-19 pandemic has led to the frequent application of telemedicine, which has been accepted by the Health Authority under the general rules for the provision of health services and the Code of Medical Ethics.

This situation has led to the identification of several areas that are emerging in the field of digital medicine, and on which regulation is necessary, which is a key challenge because it has a direct impact on the right to health and society in general.

The first issue has to do with the precision of the provision of health services and with the limitations of the applicability of telemedicine. Since there is currently no specific regulation, this scope of telemedicine is established and applied by the health professionals themselves, who must assess the relevance of its application to avoid errors in diagnosis or treatment, and to be able to establish precisely when to refrain from providing digital services.

However, digital medicine also includes the appropriate use of electronic medical records, for which appropriate technological systems, prescription tools, etc, must be applied. This is not regulated at the moment, but it is important to avoid errors and the possible liability of physicians.

It will also be necessary to regulate the responsibility of patients in complying with medical recommendations and in managing their health situation with the tools provided digitally.

In other words, digital health technology has generated the need for the regulation to change and adapt to new circumstances, with the ultimate goal of benefiting the patient.

1.5 Impact of COVID-19

Although in Ecuador there is no specific regulation on digital healthcare technologies and digital healthcare services, these have been applied for the management and control of the pandemic in all public and private health facilities.

Several advantages can be identified from this, for example:

- the use of technology allows healthcare establishments to carry out remote diagnoses and treatments, and this also avoids crowding in healthcare establishments;
- a data information-exchange mechanism has been generated, which has also made it necessary to adapt the law to the need for personal data protection; and
- technology is also used in devices for patient-monitoring, such as sensors, monitors, and medical applications – this allows precision in diagnosis or treatment.

In May 2023, the National Emergency Operations Centre (EOC) joined the declaration of the World Health Organization (WHO) regarding the end of the COVID-19 emergency. The Ministry of Health prepared a technical report that served as the basis for the conclusion that the country

has a high level of immunity, sufficient vaccine stock, and a successful immunisation process; therefore, COVID-19 is no longer considered a public health emergency in Ecuador.

Notwithstanding the above, several of the healthcare mechanisms implemented at the public and private levels during the pandemic, have already been established as common means of healthcare delivery, and this includes digital means of healthcare.

One of the advances in this sense is contemplated in the issuance by the Healthcare Authority of the Instructions for the Control of Patient User Safety Practices, which contemplates the use of physical and digital tools to ensure timely and safe access to healthcare information.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

In Ecuador, several authorities are involved in digital medicine, led by the Ministry of Public Health (MSP) and its affiliated entities, such as the National Agency for Regulation, Control and Health Surveillance (ARCSA) and the Agency for Quality Assurance of Health Services and Prepaid Medicine (ACESS).

The MSP is responsible for the exercise of the managing role in health, as well as having responsibility for the application, control, and surveillance of compliance with the Personal Data Protection Law, and whose responsibilities are detailed exhaustively in Article 6 of the aforementioned Law.

However, in Ecuador, there is also the ARCSA which has among its powers the sanitary registration of drugs and medical devices that may be useful in the field of digital medicine.

ARCSA's attributions are generally related to the application and observance of guidelines, technical regulations, standards, and protocols governing products for human use and consumption.

Finally, there is the ACESS which has among its powers:

- the control and licensing of establishments that provide healthcare services;
- the regulation, technical control and sanitary surveillance of the quality of public, private and community health services, whether for-profit or not-for-profit; and
- the control and licensing of healthcare and prepaid medicine companies and healthcare personnel.

The entity must also promote and encourage the continuous improvement of the quality of healthcare and patient safety in public, private and community healthcare services.

2.2 Recent Regulatory Developments

The regulation of digital medicine has not been developed in recent years; in fact, in Ecuador, there are only regulatory norms with vague provisions on the subject.

Until the year 2022, it was expected that the regulation in this area would advance with the issuance of the new Organic Health Code.

However, the National Assembly decided to temporarily shelve the debate related to the Health Code, so its enactment was put on hold and, to date, there is no plan to resume the approval process.

However, the entities in charge of public policy continue to make efforts in this area, one of which includes the issuance of the Ten-Year Health Plan 2022-2031 by the National Healthcare Council, an entity attached to the Ministry of Health through which the "Digital Health Commission" was created, with the aim of drafting the regulations to govern telemedicine services in Ecuador.

The Ministry of Telecommunications and the Information Society issued the Digital Transformation Agenda, one of the pillars of the Digital Culture and Inclusion Axis is Digital Healthcare. The lines of action in healthcare are:

- to build and implement a digital healthcare transformation plan;
- to implement the Single Electronic Healthcare Record and establish the interoperability of information systems in the healthcare sector;
- to promote programmes and projects in digital healthcare, considering the promotion of telemedicine services in rural areas and priority groups;
- to promote technological implementation projects to strengthen digital healthcare in Ecuador;
- to promote the use of data in the healthcare sector in order to foster research and innovation; and
- to promote inter-institutional co-operation between the public and private sectors to promote digital healthcare in Ecuador.

2.3 Regulatory Enforcement

Key Areas of Regulatory Enforcement

The provision of healthcare services and devices is currently governed by the Organic Health Law. This law determines the administrative infractions in healthcare matters, which cover aspects related to both the provision of healthcare services and the commercialisation and administration of products subject to control and surveillance.

Regarding the provision of healthcare services, the Organic Health Law covers aspects related to the authorisation of professional practice, the registration and obtaining of permits, the adequate provision of services according to the specialty, the issuance of medical prescriptions, as well as the possibility for the national healthcare authority to conduct investigations relating to illegal practices, lack of expertise, impropriety, and non-compliance, in the exercise of healthcare professions, without prejudice to the actions of the ordinary justice system.

Regarding the commercialisation and administration of products subject to control and surveillance, the Organic Health Law includes the control of drugs, medical devices, biological products, food supplements, cosmetics, etc. In general, if irregularities are found in the importation, storage, distribution, transportation, advertising, promotion or pricing of these products, the Health Authority may issue sanctions.

Sanctions under the Healthcare Law may include a fine, as well as forfeiture and/or suspension of operations or professional practices.

This law establishes that this authority may prosecute a professional or establishment ex officio or by the complaint.

Administrative Procedure

Once alleged non-compliance with the law is determined, the corresponding health authority (Commissioner, Co-ordinator or Director) will issue an initial order that will include the date and time for the trial hearing to take place.

At the trial hearing, the offender shall be heard, and shall intervene himself or herself or through his or her attorney; the evidence submitted by him or she shall be received and added to the proceedings.

If so-requested by any of the parties or ex officio, in the same proceeding, the case shall be opened for trial for a term of six days, in which all the evidence requested shall be taken.

The resolution issued may be appealed before the superior hierarchical authority in a second and final instance.

Sanctions

In sanctioning matters, in addition to the Organic Healthcare Law, the Organic Administrative Code is also applicable regarding the conduct of the administrative procedure, guarantees of due process, and the right to defence.

In this sense, the regulatory entities have issued resolutions emphasising that, in all administrative sanctioning proceedings, the alleged offender shall be guaranteed the following:

- all people maintain their legal status of innocence, and must be treated as such, as long as there is no administrative act that has caused a status in an administrative proceeding, or a duly executed judicial proceeding, that resolves otherwise;
- the alleged offenders shall be summoned or notified of the facts with which they are charged, of the infractions that such facts may constitute, and of the penalties that may be imposed, as well as the identification of the Health Authority or body competent to impose the penalty and of the rule that attributes such competence; and
- in no case shall a sanction be imposed without the duly established procedure having been followed, the omission of which would result in the nullity of the procedure.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

In these contexts, it is important to note that, for the implementation of telemedicine, the Ministry of Telecommunications and the Information Society are involved, which through Ministerial Agreement No 22, approved the Digital Transformation Agenda in Ecuador, which highlights the importance of telemedicine, indicating the following:

- In the field of digital inclusion, information and communication technologies have the potential to boost education, work and healthcare distance services.
- Currently, the implementation of regulatory frameworks that allow the inclusion of telemedicine platforms for the benefit of the patient continues to be a challenge for both the National Health System and telecommunications, but there is no regulation or limitation in the private sector.
- In recent years, certain pilot projects have been developed for the enactment of telemedicine, such as Vicente Corral Moscoso Hospital, which involved the implementation of a complete computer workstation, a high-definition plasma screen, with their respective speakers, and multi-functional printing and scanning equipment, in addition to the Call-Centre 171 for the detection of symptoms related to COVID-19.

In addition, the Ministry of Public Health, through the National Healthcare Council CONASA, is a relevant authority in this area, after the formation of the Digital Healthcare Commission, through which the new regulations on telemedicine and related aspects will be developed.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

The National Health System Law defines health services as those intended to provide healthcare, promotion, prevention, recovery and rehabilitation on an outpatient, home, or inpatient basis, classified according to their resolution capacity, levels of care and complexity.

According to this law, a clear distinction is made between preventive and diagnostic healthcare.

The Health Authority must issue a Comprehensive Health Plan, which is guaranteed by the State, as a strategy of Social Protection in Health, will be accessible and of mandatory coverage for the entire population, through public and private providers.

As far as preventive healthcare is concerned, the Integral Health Plan provides:

- a set of personal preventive benefits;
- actions for the prevention and control of risks and damages to collective health, especially related to the natural and social environment; and
- intersectoral health promotion actions, aimed at maintaining and developing healthy individual and collective conditions and lifestyles.

For diagnostic healthcare, the Integral Health Plan encompasses the activities of detection, diagnosis, recovery and rehabilitation of health as well as the provision of the necessary services, medicines, and supplies at the different levels of complexity of the system, to solve the health problems of the population at the national, regional and local epidemiological levels. The preventative and diagnostic health mechanisms are merged through the co-ordination functions exercised by the MOH, mainly as provided for in the National Health System Law and concern the following activities:

- sectoral conduction;
- sectoral regulation;
- guarantee of equitable access to healthcare;
- harmonisation of the provision of services;
- development of the essential functions of public health;
- control and evaluation; and
- any other functions assigned by the Constitution of the Republic, laws, and regulations.

In general, the Ecuadorian State is making efforts to strengthen preventative healthcare, although no great progress has been made in terms of regulation.

4.2 Increased Preventative Healthcare

The Constitution and the Organic Health Law include, as basic principles, the promotion, prevention, recovery, rehabilitation and palliative care of individuals.

The Social Security Law also contributes to this by including prevention as an important principle. For example, the laws establish that social protection will be progressively extended to the member's family and that preference will be given to risk prevention.

Though these provisions have to do with obligations imposed on employers to prevent occupational risks, they have been taken as a parameter for developing a public health policy that contributes to reducing the operation costs of the National Health System, as well as promoting social trends related to physical fitness and well-being.

The COVID-19 pandemic could also be taken as a cause for the increased attention to preventative health because it highlighted the need to optimise the performance of health professionals in such a way that they could deal with diagnosed cases that require direct attention.

Further, the implementation of a preventative health system has been facilitated by the use of technological capacity, telemedicine and a strict immunisation plan.

During the year 2022, and so far in 2023, the regulation in different matters has been updated, generating the need for preventive medicine plans to be carried out in different instances. Thus, this point has been included in the Technical Standard for the Institutional Care of Children and Adolescents, the Organic Law on Youth, and the Standard for the Protection of the Rights of Senior Citizens, among others.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

There are very specific rules to protect patient's information in Ecuador. These rules stem from the Constitution and are also reflected in the Organic Health Law, the Law on Patient Rights and Protection, the Law on the National Public Data Registry System, and even the Law on Statistics, all of which pertain to the confidential nature of citizens' health data.

The general regulation on the management of healthcare information already had several standards in force, including the following:

- In Article 66, paragraph 19, the Ecuadorian Constitution establishes as a citizen's right "the protection of personal data, which includes access and decision on information and data of this nature, as well as its corresponding protection. The collection, filing, processing, distribution or dissemination of such data or information shall require the authorisation of the owner or the mandate of the law".
- Article 7 of the Organic Health Law states that every person has the right to have a "single clinical history written in precise, understandable and complete terms; as well as confidentiality with respect to the information contained therein..."
- Article 4 of the Law on Patient Rights and Protection states that: "Every patient has the right that the consultation, examination, diagnosis, discussion, treatment and any type of information related to the medical procedure to be applied to him or her shall be confidential".
- Article 6 of the Organic Law of the National System of Public Data Registry declares confidential personal data, such as ideology, political or union affiliation, ethnicity, health status... and other data related to personal privacy [...] Access to these data will only be possible with the express authorisation of the owner of the information, by law or by court order.
- Article 21 of the Law on Statistics provides that, "Individual data obtained for statistical and census purposes are confidential [...] individual information of any kind may not be disclosed, nor may it be used for other purposes...".

However, since 2021, when the Personal Data Protection Law was enacted, specific rules on health data were incorporated, defining them precisely as sensitive because improper use could give rise to discrimination or infringe fundamental rights and freedoms.

In Ecuador, the general rule is that the processing of sensitive personal data is prohibited unless certain circumstances occur, which in the field of the handling of medical devices with AI may include the following:

- the holder has given their explicit consent for the processing of their personal data, clearly specifying its purposes;
- the processing is necessary to protect the vital interests of the holder, if the holder is not able, physically or legally, to give their consent; or
- the treatment is necessary for scientific or historical research or statistical purposes.

Thus, the institutions that make up the National Health System, physicians and companies may collect and process data relating to the health of their patients through medical devices that use AI only when the above-mentioned circumstances are met.

4.4 Regulatory Developments

Prevention is a principle related to the exercise of the right to health; however, there is no specific legislation that regulate this mechanism for the provision of health services.

In this sense, the Constitution of Ecuador recognises that healthcare is a right guaranteed by the State, whose realisation is linked to the exercise of other rights, including the right to water, food, education, physical culture, work, social security, healthy environments, and other rights that support good living.

In this sense, economic, social, cultural, educational and environmental policies; and permanent, timely and non-exclusionary access to programmes, actions and services for promotion of comprehensive healthcare should be governed by certain principles that include equity, universality, solidarity, interculturality, quality, efficiency, efficacy, precaution and bioethics, with a gender and generational approach.

Notwithstanding the above, the principle of prevention in health matters is reflected in current laws and codes such as the Organic Health Law, the Law on Patient Rights and Protection, the Law on Social Security and the Law on the National Health System.

In the area of preventive medicine, the norms revolve around the obligation of the State to guarantee immunisation against certain diseases, under the terms and conditions required by the national and local epidemiological reality. The Organic Health Law grants the Ministry of Health the competence to establish the norms and the basic national immunisation scheme, and to provide the population with the necessary elements to comply with it, at no cost.

In addition, several regulatory reforms have been created, related to the obligation of the National Health Authority to provide healthcare establishments with the biological products and supplies for the immune-preventable diseases contemplated in the basic national vaccination scheme, in a timely and permanent manner, ensuring their quality and conservation, at no cost to the end user. Likewise, at the private level, regulations have been established regarding the sanitary registration and commercialisation of biologi-

cal drugs, and the establishment of vaccination centres, etc.

From the research conducted, the Ministry of Health has the medium-term objective of issuing regulations related to preventative healthcare and, mainly through immunisations, to achieve a better quality of life, health and equity in the Ecuadorian population. The National Plan for Good Living, the Model of Comprehensive Community and Intercultural Family Healthcare (MAIS/FCI) and the principles of the Global Vaccine Action Plan were enacted towards this objective.

4.5 Challenges Created by the Role of Non-healthcare Companies

Companies not connected with the provision of healthcare services are understood to be those that offer new products, equipment or technology.

These companies must take into account that everything related to health and consumption by people requires a licence and certain individual precautions, according to the nature and operation of this new technology.

Thus, for example, in the healthcare field, all products for human use and consumption are subject to sanitary registration; devices, medicines, and equipment with new technology must comply with the Technical Regulations.

The sanctions established in the Organic Health Law may include the possibility of imposing a fine, seizing of the product, suspending operations, and temporary or definitive closure of the establishment that uses or commercialises those products.

Additionally in this area, the Law previously established that before personal data can be transferred it must be anonymised. Since this is something new, companies in Ecuador should start with a process of implementation, guarantees and publication of these conditions.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

There have been several initiatives in Ecuador, such as the use of telemedicine and the regulation and issuance of digital prescriptions during the COVID-19 pandemic, that were essential to guarantee the right to health of the population.

Additionally, Ecuador was one of the first countries in Latin America to implement the COVID-19 Auxiliary Diagnostic System, based on the Huawei Cloud in combination with AI, which was applied in the Hospital General del Norte de Guayaquil Los Ceibos and the Hospital General del Sur de Quito. This solution made it possible to diagnose more than 3,000 suspected cases per month using AI software.

This software contains thousands of images from around the world of suspicious lesions in the lungs of patients affected by COVID-19. The images are entered into the system, the results are compared and a more accurate and rapid diagnosis can be effected.

Although there is no specific standard or strategy, the Health Authority has focused its efforts on incorporating new technologies into the provision of health services and, gradually, devices with AI and other developments have become

part of daily use, not only during the pandemic bur also in other instances such as diagnostics, treatments and surgical interventions.

The use of artificial intelligence and connected devices for the diagnosis and treatment of diseases is an aspect that has been increasing in comprehensive public healthcare and in private healthcare facilities. In this sense, the Health Authority has strengthened regulations by establishing specific requirements for devices used in healthcare services.

The current regulation contemplates:

- technical Sanitary Regulations containing a specific chapter for diagnostic, treatment and digital health equipment;
- regulation of the National Public Procurement System in order to make the acquisition of these products feasible through special mechanisms applicable to healthcare facilities; and
- regulation for the provision of specialised healthcare services at home, for serious or chronic diseases.

5.2 Legal Implications

In general, health services are provided by health professionals, defined in the Organic Health Law as those whose third or fourth-level university education is specifically and fundamentally aimed at providing professionals with the knowledge, techniques, and practices related to individual and collective health and the control of its conditioning factors.

The health professions include:

- physicians;
- dentists;
- midwives;
- and others with higher technical or technological university degrees such as technologists, nurses and auxiliary health professionals.

In this sense, Ecuadorian regulations oblige doctors, nurses and auxiliary health professionals, etc, to exercise due care in the performance of their services, based on ethical standards.

Precisely on this last point, bioethics is a mechanism to be applied in the face of possible harm caused by the practice of medicine or other health professions.

In Ecuador, as in other countries, the regime that mainly addresses liability for adverse effects in the provision of health services is the criminal one, based on the Comprehensive Organic Criminal Code, particularly Article 146, which incorporates professional malpractice as a crime.

According to the described norm, persons who, by infringing an objective duty of care in the exercise or practice of their profession, cause the death of another, will face imprisonment of one to three years. If the death is caused by unnecessary, dangerous and illegitimate actions, the penalty will be imprisonment of three to five years.

This regime requires that for the determination of the infraction of the objective duty of care the following points must be noted:

- mere production of the result does not constitute an infraction of the objective duty of care;
- non-observance of the laws, regulations, ordinances, manuals, technical rules, or lex artis that are applicable to the profession;
- the harmful result must derive directly from the breach of the objective duty of care and

not from other independent or related circumstances;
- the diligence, degree of professional training, objective conditions, foreseeability and avoidability of the event will be analysed in each case.

In addition to the above, the production of adverse effects in the provision of health services also has a preventative aspect according to the Organic Health Law. In this sense, if the professional presents sufficient evidence of precaution, then criminal liability may not arise.

Article 201 of the Organic Health Law establishes that it is the responsibility of health professionals to provide quality care, with warmth and efficiency, within the scope of their competencies, seeking the greatest benefit for the health of their patients and the population, respecting human rights and bioethical principles.

Likewise, it establishes as an infraction subject to a fine, any individual and non-transferable act, not justified, that generates harm to the patient and is the result of:

- non-observance in compliance with the rules;
- impetuosity in the performance of the health professional, with total or partial lack of technical knowledge or experience;
- recklessness in the performance of the health professional with omission of the required care or diligence; and
- negligence in the performance of the health professional with omission or unjustified delay in their professional obligation.

The claims received by the Health Authorities, as well as hospitals and other health establishments, are related to surgical interventions, wrong diagnoses, and lack of delivery of medication for treatment in public hospitals; but on a few occasions, criminal actions have been initiated.

5.3 Cybersecurity and Data Protection

As explained in **5.2 Legal Implications**, Ecuador has specific rules related to the protection of patients and their personal data.

The Personal Data Protection Law addresses the issue of personal health data, which is classified as sensitive. Sensitive data is that whose exposure could lead to serious consequences of violation of rights and basic freedoms of individuals.

It is for this reason that in Ecuador, this data must be secured against unauthorised access by third parties. The general rule is that its use is prohibited, except for the following exceptions:

- the owner has given their explicit consent for the processing of their personal data, clearly specifying its purposes;
- when the processing is necessary to protect the vital interests of the holder, if the holder is not able, physically or legally, to give their consent; or
- when the processing is necessary for scientific or historical research or statistical purposes.

The Organic Law for the Protection of Personal Data clarifies the need for the consent of the owner of the data.

5.4 Proposed Regulatory Developments

The Organic Health Law is a relatively old law dating back to 2006 and, therefore, does not expressly refer to the use of AI in medical devices, telemedicine, or other aspects of telehealth, but regulates them in a general way, addressing obligations to obtain health registration, public

permits of those who distribute such products and the competence of the Health Authority to carry out control and surveillance activities.

To regulate the registration and control of medical devices, Resolution ARCSA-DE-026-2016-YMIH of the Health Regulation Agency was issued. This regulation already introduces several concepts that are related to AI, such as software comprising the equipment, components, or software of a digital computer, necessary to enable the performance of a specific task through a medical device. They are always recorded together.

According to the Health Law, compliance with health surveillance and control standards is mandatory for all institutions, agencies, and establishments that carry out activities of production, import, export, storage, in terms of support, distribution, marketing, and sale of products for human use and consumption. Given this, the concept of techno-surveillance arises with regard to medical devices, which also applies to those that are connected to the internet or any other platform.

At the Regulatory level, other regulatory efforts have been made to regulate the use of medical equipment or devices, particularly, Resolution No ARCSA-DE-003-2017-CFMR, which contains the Technical Sanitary Regulations for the Control and Operation of the National Technovigilance System (the "Technical Regulations"). The Technical Regulations) defines techno-vigilance as "the set of activities aimed at the identification, collection, evaluation, management and disclosure of adverse events or incidents resulting from the use of medical devices for human use; as well as, the identification of risk factors associated with them, to prevent their occurrence and minimise their risks".

The notification of events, adverse incidents, or healthcare alerts, is one of the responsibilities of the holders of medical device health registries, which among others includes:

- to notify the National Centre for Pharmacovigilance (CNFV) of all suspected adverse events and incidents;
- to establish and execute necessary and timely measures and actions upon suspicion of adverse events or incidents, in order to prevent in a timely manner, the risks associated with the medical devices for human use that it manufactures or markets;
- to notify on aspects that directly or indirectly influence the safety or performance of the medical devices for which they are responsible;
- to establish and implement the necessary and timely measures to minimise and prevent errors in the use of medical devices for human use, and;
- to comply with the standards and procedures established by the National Health Authority of the country regarding medical devices for human use.

As a consequence of the above, holders of health registrations for medical devices and equipment must comply with a specific process indicated in the regulations in force, in order to correctly and efficiently carry out the notifications, reports and management of information related to adverse events or incidents associated with the medical devices for human use that they manufacture, distribute or commercialise.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

The Technical Sanitary Regulations for the Registration and Control of Medical Devices defines a medical device as an instrument, apparatus, implement, machine, application, implant, reagent for in vitro use, software, material or another similar or related article, intended by the manufacturer to be used alone or in combination, for human beings, for one or more of the specific medical purpose(s) of diagnosis, prevention, monitoring, treatment or relief of disease or injury, investigation, replacement, modification or support of anatomy or a physiological process, life support or maintenance, birth control, and disinfection of medical devices.

However, with regard to software, the Technical Regulations require sanitary registration with ARCSA for software for medical devices, defined as the equipment, components or software of a digital computer, necessary for the performance of a specific task, in contrast to the physical components of the system (hardware). Medical device software will be registered under the same sanitary registry as the medical device for which it is intended to be used, as long as it is factory-conditioned with the medical device.

Regarding its classification, software for medical devices will be automatically included in the same risk level as the medical device for which it is intended to be used, and, therefore, in the same Sanitary Registry.

In general, continuous improvements made to the software must be notified to the Health Agency, in accordance with the regulations in force. In the case of a notification, they can be implemented without delay.

At the moment, any software that uses continuous or adaptive learning from AI and machine learning, as opposed to "locked" algorithms and software in software-based or software-enhanced devices, is not subject to any specific regulation.

The challenges faced by companies outside the healthcare industry in offering software as medical-device technologies are the complexity in compiling a technical dossier for sanitary registration and the lengthy registration times for these types of products.

7. Telehealth

7.1 Role of Telehealth in Healthcare

Currently, Ecuador does not have a legal framework that specifically regulates the provision of telemedicine healthcare services.

In this respect, the first requirement established for telemedicine to be provided in Ecuador is that the health professional must have a degree registered with the Ministry of Health, otherwise, he or she is not authorised to offer medical consultations or to prescribe in the jurisdiction of Ecuador.

In the private sector, the Organic Health Law and the Code of Medical Ethics must be applied, according to which telemedicine must be based on the doctor-patient relationship, confidentiality and quality of medical care, with the obligation to:

- explain the limitations inherent to the practice of virtual medicine;

- obtain informed consent from patients and/or their caregivers; and
- in cases of referral and counter-referral, deliver the complete form and data necessary to respond to the consultation (images, electrocardiogram, medical history, etc) as appropriate, with prior authorisation from the patient.

The responsibility remains the same as in face-to-face consultations. It is important to note that referrals in telemedicine (in which an international consultation may occur), will be taken as a second opinion, and the responsibility for the patient lies with the first attending physician.

The ethical standards on which telemedicine should be based remain relevant to the physician-patient relationship. Although this new mechanism of applying medicine entails new challenges for physicians, it is still based on trust, mutual respect, and the general rules established in the law for the practice of medicine.

7.2 Regulatory Environment

In Ecuador, there have been no temporary changes in the regulations related to COVID-19 regarding the provision of healthcare services. Digital medicine, and particularly telemedicine, is not prohibited.

Undoubtedly, the practice of telemedicine should be subject to specific regulations, precisely to standardise and improve these services, including the determination of appropriate platforms for the practice of digital medicine.

7.3 Payment and Reimbursement

There are no specific rules or private guidelines to follow in the field of telemedicine.

However, chapter VIII of the Code of Medical Ethics does describe the general regulation of medical fees, establishing that equity is the first and most universal moral norm for collecting professional fees; they must pay close attention to fairness, local customs, the magnitude of service, to the prestige and necessity of personal intervention, to the economic conditions of the patient and any honest pre-established pact, if there is one.

This code establishes that free care will be detrimental to colleagues and must be limited to cases of close kinship, assistance to colleagues, and manifest poverty. In this respect, in cases in which a patient, without justified reason, refuses to comply with the pecuniary commitments with the physician, the latter, once all private means have been exhausted, may demand payment of fees without affecting, in any way, the good name or credit of the plaintiff.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

The incorporation of various technologies into medical devices has grown significantly. These technologies have improved the conventional functions and operation times of medical devices, as well as offering new and innovative functions.

Technological developments in electronics, mechanics and computer systems have made it possible to include wireless technology in medical devices, as well as many different functions linked to the diagnosis, treatment, control and monitoring of patients' health to be included in medical devices, which has optimised these

devices. Some of the new functions made possible by wireless technology are the transfer and processing of data in real time, which allows for faster diagnosis and monitoring, the restriction of access to unauthorised personnel through fingerprint or facial recognition, protection against data manipulation (data integrity), and the administration of drugs according to the data that the device has obtained automatically, or has been assigned to it, etc.

Ecuadorian regulations for medical devices recognise as medical devices both individual software and devices that have coupled software systems.

ARCSA establishes that medical devices must obtain a sanitary registration before being marketed in Ecuador. To obtain a sanitary registration, ARCSA evaluates the quality, safety and efficacy of the finished product for its purpose.

Devices that use software linked to the internet require system updates, and are susceptible to computer viruses (malware), or to suffering cyber-attacks. This can impact the quality, security and efficiency of the device.

Currently, ARCSA regulates the following categories of products for human use and consumption: medicines, natural products, food, cosmetics, household and industrial hygiene products, and medical devices.

The digital assistant Alexa does not fit into any of the aforementioned categories; therefore, Alexa does not need to comply with any regulations.

"Medical devices" for human use are articles, instruments, apparatus, appliances, devices or mechanical inventions, including their components, parts or accessories, manufactured, sold or recommended for use in the diagnosis, curative or palliative treatment, prevention of diseases, disorders or abnormal physical conditions or symptoms, to replace or modify the anatomy or a physiological process or control it. These include amalgams, varnishes, sealants and similar dental products.

A "medical device" is also an instrument, apparatus, implement, machine, appliance, application, implant, in vitro reagent, software, material, or another similar or related item, intended by the manufacturer to be used alone or in combination, for human beings, for one or more of the following specific medical purposes:

- diagnosis, prevention, monitoring, treatment, or relief of a disease;
- diagnosis, monitoring, treatment, relief or compensation of an injury;
- investigation, replacement, modification or support of the anatomy or of a physiological process;
- life support or maintenance;
- birth control;
- disinfection of medical devices; and
- provision of information by in vitro examination of samples from the human body and does not exert the primary action intended by pharmacological, immunological or metabolic means, in or on the human body, but may be assisted in its function by such means.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

In telecommunications, 5G is the acronym used to refer to the fifth generation of mobile telephone technologies.

The use of this technology is provided for in the National Telecommunications and Information Technology Plan, issued through Ministerial Agreement No 7 dated 24 June 2016.

With the use of 5G technology, healthcare delivery systems will be able to enable mobile networks to manage telemedicine better, as well as to assign appointments, manage medical records, etc.

In other words, the implementation of 5G systems can contribute to the ultimate goal of facilitating the reach of telemedicine programmes to a larger number of patients and in various specialisms.

In addition, Ministerial Agreement 015-2019 approved the Ecuador Digital Policy, which aims to transform the country towards an economy based on digital technologies, by reducing the digital divide, developing the information and knowledge society, digital government, efficiency in public administration and digital adoption in social and economic sectors.

The Ecuador Digital Policy is mandatory for the public and private sector, related to the general telecommunications society, information society, information technology, information and communication technologies, postal and civil registry, and information security.

The implementation of this policy will be based on three main lines of action: connectivity, efficiency and security of information, and innovation and competitiveness, with the following health impacts:

- strengthening the interoperability of state healthcare providers with new digital technologies; and
- encourage spectrum bidding for new bands for the "massification" of 4G and deployment of 5G, promoting emerging technologies such as the internet of things and big data.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

One of the key issues when discussing the provision of personal data in clinical or research settings lies in the treatment and use that will be given to that data.

In this respect, the key points will be prior consent, except in cases of urgency, confidentiality and professional secrecy, in the handling of any such data.

In this regard, the recently published Personal Data Protection Law determines that health-related data contained in the institutions that make up the National Health System may be processed by private and public natural and legal persons for scientific research purposes, provided that, as the case may be, they are anonymised, or the processing is authorised by the Personal Data Protection Authority, following a report from the National Health Authority.

The exchange of data, and, in general, its treatment, may be carried out in the following cases:

- by consent of the holder for the processing of his or her personal data;
- where it is carried out by the data controller in compliance with a legal obligation;
- where it is carried out by the data controller, by court order;

- where the processing of personal data is based on the fulfilment of a mission carried out in the public interest or in the exercise of public powers vested in the controller;
- for the execution of pre-contractual measures at the request of the owner of the data or for the fulfilment of contractual obligations pursued by the data controller, data processor or by a legally authorised third party;
- to protect vital interests of the owner of the data or another natural person, such as their life, health or integrity;
- for the processing of personal data contained in publicly accessible databases; or
- to satisfy a legitimate interest of the data controller or a third party, provided that the interests or fundamental rights of the owner of the data do not prevail under the provisions of this regulation.

De-identification is applicable only when the health-related data contained in the institutions that make up the National Health System are processed for scientific research purposes, provided that, as the case may be, they are anonymised, or any such processing is authorised by the Personal Data Protection Authority, following a report from the National Health Authority.

Given the recent enactment of the Personal Data Protection Law, there is still no regulation on medical research when the comparison of anonymised data with other data sources may result in a re-identification, because health data is personalised.

Consent has also been the subject of express regulation, which must comply with the following conditions: it must be freely given, specific, informed and unambiguous.

The application of the conditions for consent, use and processing of personal and sensitive data must be complied with at all times in the field of digital healthcare; there are no exceptions deriving from the use of portable devices.

In the event of non-compliance with the provisions set forth in the Personal Data Protection Law, whether in the healthcare field or any other, the Personal Data Protection Authority will issue corrective measures, with the aim of preventing the infringement from continuing and the conduct from happening again.

Corrective measures may consist of, among others:

- the cessation of the processing, under certain conditions or deadlines;
- the deletion of the data; and
- the imposition of technical, legal, organisational or administrative measures to ensure proper processing of personal data.

Notwithstanding the foregoing, these may also be considered criminal offences.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

The use of AI in digital medicine is a particularly useful tool for meeting the demand for services and facing the challenges that this represents in the healthcare system. This is due not only to the use of digital medicine, but also to the complexity of the treatments and the tools or inputs required to execute them.

It could be stated that Ecuadorian health legislation has indirectly regulated medical equipment

that uses AI; however, they are placed in a similar condition to any biomedical input or device, which can generate complications at the time of presenting requirements for obtaining sanitary authorisations. There are also directions on their proper use and on carrying out the subsequent controls to which they are normally subject.

11.2 AI and Machine Learning Data Under Privacy Regulations

When we talk about AI, general legal knowledge is required in the pharmaceutical, sanitary, IP, and compliance fields, taking care that all the control areas are covered to avoid risks and that there are adequate practices in the distribution, use, personal data protection, patient protection, competition, among others.

AI has been used in products in active medical devices, such as a compact battery-operated devices used for endoscopic procedures, an assisted surgery system that can locate anatomical structures in open interventions, and systems used in orthopaedic surgery.

The rules that are mainly applicable to the sale and use of these devices have their starting point in the Organic Health Law, and later regulatory standards such as the Technical Regulations for Registration and Control and the Pharmacovigilance Regulations, Resolutions, and Instructions.

However, one of the most novel issues that differentiates medical devices that use AI from other common medical devices is the need to obtain special authorisations, such as in the field of telecommunications. Requirements include:

- permits from the Personal Data Protection Authority for the protection of personal data;
- protection of new technologies; and
- incorporation of restrictions for access to data.

Regarding data protection, there is no specific regulation for medical devices with AI, but in 2021 the Organic Law on Personal Data Protection was issued, which introduced to Ecuador the rights related to data protection, including informed consent, rectification, updating, deletion, opposition, cancellation and portability.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Among the regulatory and legal problems faced by companies that develop and sell new digital technologies for healthcare, the following should be noted.

In the health field, all products for human use and consumption are subject to sanitary registration. Products that deal with new technologies, for example, AI or software, are regulated by a Resolution of the Regulatory Agency, about which it is important to take into account that in Ecuador software cannot and does not require a sanitary authorisation to be used.

For the protection of sensitive personal data, companies must ensure that each device, device, and/or piece of software includes an informed, prior, complete and specific consent in which exactly what information can be collected and who will be responsible for its handling is defined.

In this area, additionally, the Ecuadorian law establishes that for the transfer of personal data a previous condition of anonymisation of the information must be fulfilled, so it is necessary,

being something new, that the in Ecuador start with a process of implementation, guarantees, training and publication of these conditions, among others.

The regime of corrective and sanctioning measures of the Personal Data Protection Law, which includes fines, came into force on 26 May 2022.

Finally, although it is not mandatory, it is recommended that companies begin to require intellectual property protection of software through copyrights, since the Code of Ingenuity protects them as literary works, regardless of whether they have been incorporated into a computer or whatever the form in which they are expressed.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

The Vice Ministry of Telecommunications and Information and Communication Technologies has stated that establishing public policies in the telecommunications and information society sector is a first step toward promoting the development of telecommunications and ICT in Ecuador, in order to generate confidence in the markets at the regional level, as well as to improve competitiveness, ensure growth and extension, through the use of technology and various applications, and to have a population trained in the efficient use of ICT. The next step is the implementation of these policies through the Information and Knowledge Society Plan, which seeks to define a strategic framework to articulate the efforts of the different participants, in order to achieve the proposed objective.

On 7 February 2023, the Organic Law for Digital and Audiovisual Transformation was enacted, which establishes the general guidelines for digital transformation.

The Digital Transformation constitutes the continuous process of multimodal adoption of digital technologies that fundamentally change the way in which government and private sector services are conceived, planned, designed, implemented and operated, in order to improve the efficiency, security, certainty, speed and quality of services, optimising their costs and improving the conditions of transparency of the processes and actions of the State in its interrelation with citizens.

One of the objectives of this Law is to establish the regulatory framework for the promotion of the digital transformation of public institutions, private companies and society; as well as to strengthen the effective and efficient use of platforms, digital technologies, networks and digital services in order to attract investments, boost the digital economy, efficiency and social welfare, developing digital skills and competencies necessary for employment, education, healthcare and productivity.

Once this law has entered into force, it is estimated that in the short term a regulatory framework will be established to promote the digital transformation of public institutions, private companies and society; as well as to strengthen the effective and efficient use of platforms, digital technologies, networks and digital services in order to attract investment; boost the digital economy, efficiency and social welfare; and ensure that the digital skills and competencies necessary for employment, education, healthcare and productivity are developed.

13.2 Data Management and Regulatory Impact

The updating of systems and software of any kind brings with it two problems that have had to be resolved in the legislation. The first is related to the control of updates made to medical device software, since they are not obliged to be subject to prior approval by the Health Authority.

The second problem is the proper handling of the data that is part of the system that is intended to be updated, which may include personal data that identifies or makes identifiable a natural person, directly or indirectly. Sensitive data includes everything related to the physical or mental health of a person, including the provision of healthcare services that reveals information about their state of health.

In the first case, the Health Authority has implemented control and surveillance mechanisms, established in the Organic Health Law, which give the Health Authority the power to carry out an inspection of equipment and its software at any time. The Health Authority may order the suspension of marketing and use of the product and impose sanctions such as fines and retention.

Another of the control mechanisms is technosurveillance, regulated by the Technical Regulations and used for the identification, collection, evaluation, management and disclosure of adverse events or incidents resulting from the use of medical devices of human use, as well as the identification of the risk factors associated with them, to prevent their use and minimise their risks.

On the other hand, health data management involves the collection and storage, quality control, processing, and compilation and analysis of the data and is regulated by the Personal Data Protection Law.

In this sense, Article 30 of this Law establishes the following relevant points that must be taken into account when updating IT and in the management of health information in general.

- The National Health System and health professionals may collect and process data relating to the health of their patients who are or have been under their treatment.
- Those responsible for and in charge of data processing, as well as all persons involved in any phase thereof, will be subject to the duty of confidentiality.
- The consent of the owner will not be required for the processing of health data when this is necessary for reasons of essential public interest in the field of health.
- The consent of the owner will not be required when the treatment is necessary for reasons of public interest in the field of public health, as in the case of serious cross-border threats to health, or to guarantee high levels of quality and security of the data.

14. Intellectual Property

14.1 Scope of Protection

The scope of protection of patents is determined through their claims.

The scope of copyright protection is in the creation of the idea or literary work, where the software is included.

The scope of protection of trade secrets is materialised through a contract or agreement that determines that the information is confidential

and therefore is contained in trade secrets that no one can share.

In reference to databases, the INGENIOS Code states: "Compilations of data or other materials, in any form, which for reasons of the originality of the selection or arrangement of their contents constitute creations of an intellectual nature, are protected as such. This protection of a database does not extend to the data or information collected, but it will not affect the rights that may subsist on the works or services protected by copyright or related rights that comprise it".

In this respect, the scope of protection of the database has been established since its creation, provided that it is of an intellectual nature.

Regarding the work's authorship, Ecuadorian law specifies that only a natural person can be the author; so, when talking about a technological device that does not have direct human contributions, its creations will be owned by the natural person who created the technological device. However, in the event that this creation has been by mandate of a company, it may claim its economic rights, if they are detailed in the contract for the provision of services.

14.2 Advantages and Disadvantages of Protections

Copyright

Advantages

Copyright allows the protection of audio-visual works, illustrations, graphics, designs, software, among others. Having protection can prevent unauthorised third parties from making use of the creation.

Disadvantages

With the constant advancement of technology and the emergence of new devices for digital medical care, it is possible that the current legislation does not contemplate the new rights.

Industrial Property

Advantages

Through trade mark protection, it is possible for each device or any platform for digital healthcare to have protection. On the other hand, it is possible to protect industrial designs that meet legal requirements through patents. In these cases, it is also possible to prevent third parties from using the owner's industrial property rights without prior authorisation.

Disadvantages

Industrial property rights, being territorial, allow trade marks or designs to be copied and registered in other countries. The registration of industrial property rights takes an extensive time that does not allow immediate protection of the right.

Being a recent issue in Ecuador, there is no judicial decision or regulatory resolution on the applicability and scope that the rights that protect the devices and structures of digital medical care will have.

14.3 Licensing Structures

In Ecuador, no structure has been specified for licensing contracts used for digital healthcare. However, Article 81 of the INGENIOS Code specifies what technology transfer will consist of as part of a process of social innovation. Similarly, as for the software used, it may be subject to a copyright licence.

The protection of digital healthcare rights can encompass a large part of intellectual property rights. Therefore, a licence will be granted for each of the rights that are intended to be

licensed, thus allowing the rights of the owner not to be infringed.

14.4 Research in Academic Institutions

The INGENIOS CODE provides that: "In the case of works created in educational centres, universities, polytechnic schools, technical, technological, pedagogical, arts institutes and intellectuals and public research institutes as a result of their academic or research activity such as degree works, projects of research or innovation, academic articles, or others analogous, without prejudice to the fact that there may be a dependency relationship, the ownership of the economic rights will correspond to those of the authors. However, the establishment will have a free, non-transferable and non-intellectual licence for the non-intellectual use of the work for academic purposes."

In relation to intellectual property rights when a company is in the private sector, the ownership corresponds to the author of the work, and the private company that collaborates with the investigation will have the quality of co-author of the work, since it would be a work in collaboration, as provided in Article 112 of the Organic Code of the Social Economy of Knowledge, Creativity and Innovation.

14.5 Contracts and Collaborative Developments

In Ecuador, there is the figure of works created under a relationship of dependency or commissioned works, which indicates that, unless otherwise agreed, the ownership of such works will correspond to the author. In this regard, in practice, companies develop specific contractual clauses on the ownership of a work or inventions, so that the company is always the owner of the rights developed by a third party under a dependency relationship.

15. Liability

15.1 Patient Care

According to the Code of Medical Ethics, healthcare professionals assume the responsibility of enforcing the Constitutional guarantee of the Right to Health of Ecuadorians.

However, in the exercise of the profession, as well as in the development of digital medicine, healthcare professionals assume a legal responsibility that should be considered with special caution when using AI for diagnostic or treatment purposes, as legal definitions relating to breach of the objective duty of care in the exercise or practice of medical care are in force in the legislation; these legal definitions can even lead to criminal liability.

In this sense, there are no grounds for exemption from liability considering only the use of AI, although it could be determined that the physician's liability could only be generated if the equipment or device that uses AI was used differently from the manufacturer's recommendations, either on the label or on the packet insert.

In other words, manufacturers and suppliers of diagnostic and treatment equipment could also have administrative and even criminal liability due to a system failure that causes damage to a patient's health.

In any case, healthcare professionals must comply with the objective duty of care and maintain prior and informed consent of the patient, which also includes the knowledge, use and eventual transmission of their personal data or sensitive data.

Developers of software or equipment with AI should consider the new regulations in Ecuador

regarding the protection of personal data and the Law on Patient Rights and Protection, to take care of any legal liability that may arise from the use of the software.

15.2 Commercial

In the healthcare field, the duty of safety and responsibility has a very extensive content. In a broad sense, it implies the obligation of the external provider of services and goods to allow access to healthcare entities whose quality, safety and efficacy guarantee the health and physical integrity of the consumer/patient.

Thus, the Constitution of the Republic obliges them to guarantee the quality of goods and services offered to consumers and establishes the liability of those who make an attempt against the health and safety of these.

That is why the liability for defective products (issued with “defects” allowing cyber-attacks or others) arises as a result of the duty of safety that consumer-protection rules impose on producers and suppliers in the market.

FRANCE

Trends and Developments

Contributed by:
Catherine Mateu
Armengaud Guerlain

Armengaud Guerlain was founded in 1993, and specialises in intellectual property (patents, trade marks, designs and models, and copyright) and the related issues of unfair competition, consumer law, advertising rights (particularly comparative advertising), and the internet. Reflecting its well-recognised expertise, the firm has worked with a wide variety of French and international clients, from artists and inventors to blue-chip companies, governments, and state-owned enterprises. In addition to French, the firm's daily working languages include English and Spanish. Armengaud Guerlain works with a network of foreign colleagues selected for their high level of technical expertise and their use of complementary work methods, thereby enabling the firm to manage files simultaneously in several countries. Each file is treated in a collaborative manner and the firm places particular emphasis on maintaining lasting, high-quality relationships with its clients, combining competence and reactivity.

Author

Catherine Mateu is a partner at Armengaud Guerlain with more than 20 years of experience in French and European intellectual property law, serving clients that range from inventors, designers, non-profit groups and local start-ups to multinational corporations. Her practice focuses on finding innovative, timely and cost-effective solutions to a wide array of patent, copyright, trademark, design infringement and licensing matters, as well as strategic advisory. Catherine is a regular speaker at intellectual property conferences, and is ranked in Intellectual Property: Patents in Chambers Global. She is Chair of the TRIPS Committee of AIPPI and Chair of the Emerging Issues Committee of INTA. Catherine is a native speaker of French and Spanish, and is fluent in English and Basque.

Armengaud Guerlain

12 avenue Victor Hugo
75116 Paris
France

Tel: +33 1 4754 0148
Fax: +33 1 4054 7857
Email: contact@armengaud-guerlain.com
Web: armengaud-guerlain.com

The New World of Digital Health

In 2019, the French "health unicorn", Doctolib – the largest digital health service in Europe – raised EUR150 million through funding, raising the company's value to over a billion euros. Doctolib joined forces with the elite group of other online health services, such as Peloton and 23andMe, solidifying its place in both healthcare booking, and software provision. Once again, French tech is rising in Europe, showing that its talent, as well as its financial and legal systems, are ideal for health progress and efficiency. Currently, France is expanding on the foundational need for telemedicine as an essential tool in post-pandemic Europe – saving doctors time with administrative tasks, reducing missed appointments and increasing the amount of patients that are able to be cared for. While the world of digital health is quite new – and at times can seem threateningly powerful – there are many national regulations in place to ensure safety, confidentiality, and overall the promise of impactful medical assistance.

The legislation set forth by the European Union impacts the liability for injuries that are suffered through the product-use that digital health services provide, entailing that digital health services comply with the international standards of pharmaceutical regulation. This is done by the National Agency for Medicine and Health Products Safety (ANSM), whose power includes regulating the manufacturing of pharmaceuticals, and investigation or inspection. Setting up bodies to monitor life science products placed on the market ensures the safety and compensation of victims, allowing the public to use digital health services without worry. These preventative measures extend to the requirement for life science companies to provide warning of side effects, as well as instructions, on sold or over-the-counter prescriptions. For pharmaceuticals directly prescribed by doctors, doctors may be held liable for medicine prescribed, and must assess patients based on a benefit/risk ratio.

In order for French tech to be able to properly provide its services to Europe's world of digital health, innovative software that records and assesses personal health information is provided to digital health users. According to the EU's General Data Protection Regulation (GDPR), any data that concerns health is considered sensitive data and the processing of such data is prohibited, unless it is necessary for reasons of public interest – developments in exactly what qualifies as a public interest reason is something all digital health organisations are obliged to follow very closely.

Generally, digital health providers are required to protect themselves as well, enforcing typical waivers of liability upon the patients that

use their services, especially in cases in which patients may refuse to follow the medical advice provided by the physicians and hospitals. It is through these regulations that both patients, and providers, are protected – and it is what keeps digital health services at the forefront of practical assistance in the medical field. With the legislation in place, both provider and patient can be sure that there is a safe and protected relationship between the two, furthering the medical field for the better.

Since the relationship of safety has been established in the world of digital health, it is important to understand the need for digital health, in order to expand the world of medicine as a whole. Connected medical devices have completely altered the way in which both doctors and researchers are able to use patient data in order to capture medically relevant information, to further research cures, and to allow pharmaceutical development. Patents play a large role in this allowance, as technology adoption furthers the delivery of efficient healthcare services such as wearable devices to monitor accurate data in real time. These wearable devices connect the technological world of intellectual property with the medical need to monitor disabilities and detect chronic disease as well – invaluable aspects of the modern medical world. Furthermore, the protection of these intellectual property rights goes beyond simply backing up the digital health companies, but in fact secures the protection of the rights of the individuals using the services as well. It is in this notion that the combination of digital health technology within the medical world serves a purpose that is both beyond expectations, yet was also an inevitable destination.

The world of digital health has surpassed the expectations of prior decades – it continues to allow the furtherance of medical discoveries; and to save lives. In using the data set forth by patients, digital health companies can deliver a current reality of furthered research and better healthcare, and promise a future of endless possibilities for medical discovery. With both the companies and the patients being protected by the litigation of the European Union, digital health companies are the safe and secure future of medicine.

INDIA

Law and Practice

Contributed by:
Anoop Narayanan and Sri Krishna
ANA Law Group

Contents

ANA Law Group is a full-service law firm based in Mumbai. Its team of experienced and committed professionals has broad industry knowledge and specialises in a wide spectrum of the law. Founded on traditional values and with prominent cross-border exposure, the firm has significant experience in counselling international clients on data protection and privacy in India, acting for many businesses in complex transactions. ANA Law Group has in-depth knowledge of all sectors of industry, such as banking and insurance, financial institutions, luxury goods, consumer goods and healthcare. The firm assists international companies on global privacy law involving Indian projects, drafting and negotiating contracts with their Indian counterparts, preparing data protection and privacy policies for those companies' Indian subsidiaries, compliant with major international privacy laws. Specifically, the firm advises clients on data processing and all aspects of data security, including handling cross-border data flows, security breaches and compliance with all regulatory requirements.

Authors

Anoop Narayanan is the founder of ANA Law Group and a leading Indian lawyer in corporate law, intellectual property law and information technology with three decades of experience as an attorney. Focusing on a broad range of intellectual property, IT, outsourcing, employment, technology, data protection, telecommunications and entertainment law matters, his practice encompasses both litigation and commercial or transactional advice. He has worked with India's highest-profile companies, as well as global corporates in the manufacturing, banking and finance sectors and telecommunications and technology companies. His experience and expertise in TMT and data privacy was invaluable in setting up the Indian operations of large global technology companies and handling several India-bound outsourcing transactions with the major Indian IT companies.

Sri Krishna is an associate at ANA Law Group working in its TMT and IP practice group. He regularly advises international clients on intellectual property, healthcare and pharmaceuticals-related issues in transactional, compliance and regulatory matters.

ANA Law Group

7th Floor Keshava
Bandra Kurla Complex
Bandra East
Mumbai
400 051
India

Tel: +91 22 6112 8484
Fax: +91 22 6112 8485
Email: anoop@anaassociates.com
Web: www.anaassociates.com

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

"Digital health" and "digital medicine" have been gaining traction in India over the past couple of years, particularly due to the COVID-19 pandemic; however, from a legal and regulatory perspective, they remain undefined under existing Indian laws. Digital health, as defined by the World Health Organization, is understood as a broad umbrella term encompassing eHealth, as well as emerging areas, such as the use of advanced sciences in big data, genomics and artificial intelligence. The digital health platforms include the information and communication tools (digital medicine products) used for improving and enhancing healthcare services.

1.2 Regulatory Definition

Existing Indian laws do not define the terms "digital health" or "digital medicine". However, the proposed law in this regard, which is the Digital Information Security in Healthcare Act 2018 (the DISHA Bill), defines "digital health data" as an electronic record of health-related information about an individual, including information regarding:

- an individual's physical and mental health condition;
- health service provided to an individual;
- the donation by an individual of any body part or any bodily substance;
- testing and examination data of an individual's body part or bodily substance;
- data collected in the course of providing health service to an individual; or
- details of the clinical establishment accessed by an individual.

Further, the Telemedicine Practice Guidelines (TPG), issued by the Indian government in March 2020, has adopted the World Health Organization's definition of telemedicine as "The delivery of healthcare services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of healthcare providers, all in the inter-

ests of advancing the health of individuals and their communities."

1.3 New Technologies

The following are some of the key emerging technologies in India in the field of digital healthcare.

Telemedicine

There has been significant growth and advancement in the field of telemedicine in India. This includes the use of information and communications tools for healthcare services with the virtual presence of both the patient and the healthcare provider. The tools are used for carrying out technology-based patient consultation communication via video, audio and text. The Ministry of Health and Family Welfare of India (MoHFW) issued the TPG in March 2020.

Wearable Devices

India has witnessed a tremendous increase in the use of wearable devices for health monitoring. Although these digital technologies have existed and have been used for several years, their use for more specific purposes, and also as an alternative to conventional physical health monitoring, has increased because of the COVID-19 pandemic. The preliminary screening of one's health data without having to visit a hospital or a diagnostic centre has bolstered the growth and prominence of digital technologies. Several wearable devices are now available in India, featuring heart-rate trackers, blood oxygen-level trackers, and other devices including water consumption, weight, sleep, and diet monitors.

Online Pharmacies

There has been a significant rise in the number of online pharmacies delivering medicines to patients' homes in India, more so during the pandemic.

Artificial Intelligence

AI-based systems have witnessed significant growth in India for the diagnosis of disease and also for treatment purposes.

1.4 Emerging Legal Issues

One of the major emerging issues is that the increasing number of digital and other new technologies in the healthcare industry is giving rise to concerns about data protection and the privacy of patients.

Although most of the data collection, storage and usage by healthcare providers complies with India's applicable data privacy laws, there are critical issues on the misuse of this data for other commercial purposes and also on the breaching of privacy obligations. The absence of adequate training and awareness building with regard to aspects of data privacy among the people collecting, processing and handling such data on the digital health platform also aggravates the situation.

Additionally, the absence of a specific law to regulate these aspects is a major concern. Although the MoHFW has issued the DISHA Bill, it has not yet become law. The DISHA Bill proposes to establish national and state health authorities to enforce privacy and security measures for health-related data. Further, the MoHFW has issued a Health Data Management Policy to promote the National Digital Health Mission, which lays down principles for the protection of an individual's digital health data privacy.

1.5 Impact of COVID-19

COVID-19 has led to a significant rise in the adoption and use of digital healthcare technologies in India, especially in the area of telemedicine. As non-COVID-19 patients were forced to stay at home during the nationwide or state-

specific lockdowns, healthcare practitioners provided remote consultations with the help of video/audio calls and text messages.

Technology-based consultations and remote monitoring and treatments were also extended to COVID-19 patients with mild symptoms and where hospitalisation was not required. As one of the measures to support telemedicine, the MoHFW issued the TPG in March 2020 as a temporary measure and allowed home delivery of medicines. The Indian government also developed a mobile application, Aarogya Setu, to trace COVID-19 hotspots in India and the number of people affected by COVID-19 in a particular user's geographical area. The government has also recently introduced another digital application, the CO-WIN portal, to carry out the COVID-19 vaccination drive in India.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

The MoHFW

The MoHFW is the apex authority in the organisational structure of the healthcare system in India. The MoHFW is comprised of two departments, (i) the Department of Health and Family Welfare (DoHFW), which is responsible for organising and delivering all national health programmes; and (ii) the Department of Health Research, which is responsible for the promotion of health and clinical research, development of health research and ethics guidelines, grants for research training, etc, in India.

The AYUSH

The Ministry of Ayurveda, Yoga and Naturopathy, Unani, Siddha and Homeopathy (AYUSH) develops and promotes research in alternative medicine practices. The central government's responsibilities include policy making, planning, guiding, assisting, evaluating and co-ordinating the work of the various state-level health authorities, and providing funding to implement national health programmes.

The Central Drugs Standard Control Organisation (CDSCO)

The CDSCO is the National Regulatory Authority of India and is responsible for the approval of drugs, conducting clinical trials, laying down the standards for drugs and control over the quality of imported drugs in India. The Drug Controller General of India (DCGI) is the head of the CDSCO and is responsible for licensing and controlling the functions of the CDSCO. The National Medical Commission and the National Health Authority (NHA).

The recently constituted National Medical Commission (NMC) regulates and governs medical practice in India. Besides these, the MoHFW has recently established the NHA, which is the apex body responsible for implementing public health assurance schemes, to develop strategy, build healthcare technological infrastructure and implement the "National Digital Health Mission" in India.

The Ayushman Bharat Digital Mission (ABDM)

MoHFW introduced the National Digital Health Mission (NDHM) on 15 August 2020 to create a digital health ecosystem, and recently renamed it as Ayushman Bharat Digital Mission (ABDM). ABDM aims to develop the backbone necessary to support the integrated digital health infrastructure of the country.

The following are the main components of ABDM:

Under ABDM, every citizen gets a unique health account (Ayushman Bharat Health Account), which acts as a digital repository of all health-related data of an individual. The ABHA ID is voluntary and free of cost, and enables access and exchange of health records of citizens with their consent. It also enables interaction with participating healthcare providers, and allows the participants to receive their digital lab reports, prescriptions and diagnosis from verified healthcare professionals and health service providers. It has been reported that, to date, over 38 crore ABHA IDs have been created and 26 crore health records digitally linked under ABDM.

The Healthcare Professionals Registry (HPR) under ABDM is a comprehensive repository of all healthcare professionals involved in the delivery of healthcare services across both modern and traditional systems of medicine. Enrolling in the HPR enables them to connect with India's digital health ecosystem.

The Health Facility Registry (HFR) is a repository of health facilities across different systems of medicine. Participating entities of the ABDM must register as a healthcare provider. It includes both public and private health facilities, such as hospitals, clinics, diagnostic laboratories and imaging centres, pharmacies, etc.

The ABHA mobile app will have electronic records of health-related information that conform to nationally recognised interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual. Such information can be fully controlled by the individual.

Unified Health Interface (UHI)

UHI is a network of open protocols that facilitate interoperability in health services. Through UHI-enabled applications, patients can search for, book and pay for services offered by a variety of participating providers from any application of their choice.

UHI Services

The services under UHI will include teleconsultation to book an online consultation with any doctor; booking physical appointments; discovering availability of critical care beds; booking of home visits for lab sample collections; and booking an ambulance.

The ABDM has recently launched a new initiative that has revolutionised the way patients register for Outpatient Department (OPD) services at hospitals in India. The new initiative enables patients to use their smartphones to scan a QR code and share their verified demographic data with hospitals' Health Management Information Systems (HMIS) with just one click. This has drastically reduced the waiting time for patients and ensured accurate data entry into the HMIS, doing away with the need for patients to stand in long queues.

The National Pharmaceuticals Pricing Authority

The National Pharmaceuticals Pricing Authority is the authority for controlling and monitoring the prices and availability of medicines.

State-Level Authorities

At the state level, each state has a separate MoHFW, Directorate of Healthcare Services and DoHFW, which are responsible for organising and delivering healthcare services, consisting of participants from both the public and private sectors. The State Drug Standard Control Organisation (SDSCO) is responsible for regulation of the manufacture, sale and marketing of drugs in each Indian state.

The organisational structure consists of administrative subordinate offices at regional/zonal, district and sub-district level. The public healthcare system consists of primary (community health centres), secondary (sub-district hospitals), and tertiary (district hospitals and medical colleges) care centres. Primary and secondary care hospitals are in the public sector, whereas tertiary care hospitals are in either the public or private sector. Apart from these, there are several clinics and diagnostic centres set up by individual medical practitioners.

The services provided by the private sector are registered and regulated under national/state councils constituted under the Clinical Establishment (Registration and Regulation) Act 2010, while the public sector comes under the authority of the MoHFW and state health ministries. At the district level, local self-government institutions (Panchayati Raj) are responsible for establishing primary health centres in rural areas.

2.2 Recent Regulatory Developments

The following are the key regulatory developments pursuant to the rise of digital healthcare in India and which are expected to have the biggest impact on the governance and growth of digital healthcare.

- The Indian government issued the Telemedicine Practice Guidelines (TPG) in March 2020, which cover the norms and standards of registered medicine practitioners to consult patients via telemedicine. Telemedicine includes all channels of communication with the patient that leverage information technology platforms, including voice, audio, text, and digital data exchange.
- The proposed DISHA Bill in 2018 is to standardise and regulate the processes related to the collection, storing, transmission and use of digital health data, and to ensure the reliability, data privacy, confidentiality and security of that digital health data.
- The government also issued the Health Data Management Policy in October 2020 to impose standards for data privacy protection in India.
- In April 2022, after receiving the public comments, the NHA released a Draft Health Data Retention Policy (HDR Policy) for further consultation. The HDR Policy aims to create a uniform system governing the operation of data fiduciaries, data processors, health information providers/users and data repositories within the National Digital Health Ecosystem.

These regulations will address many ambiguities from the legal, regulatory and compliance perspectives, for service providers as well as consumers. More accountability, governance and grievance-redressal mechanisms, which have comparable speed, ease and efficiency to that of the digital healthcare services, are some other primary needs for this sector.

2.3 Regulatory Enforcement

The MoHFW enforces laws relating to healthcare in India. The National Medical Commission enforces the provisions related to medical education and practice under the National Medical Commission Act 2019.

The CDSCO and the SDSCO enforce regulations relating to the manufacture, distribution and sale of drugs and cosmetics under the Drugs and Cosmetics Act 1940 (D&C Act). The central government can confiscate, regulate, restrict or prohibit the manufacture, sale or distribution of some drugs and impose a ban on certain drugs. The court can further impose penalties and imprisonment for offences under the D&C Act.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

Currently, there are no digital healthcare-specific non-healthcare regulatory agencies.

The new healthcare technologies, while providing fast and convenient services to consumers, also pose several questions and concerns. In addition to the protection under consumer protection laws, more specific regulatory regimes with respect to data privacy and an expert regulatory body in each state, as well as at the national level for grievance redressal, are some of the immediate requirements.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

Preventative and Diagnostic Care Systems

Preventative care includes services such as routine health screenings and check-ups that detect health issues at an early stage. Preventive health check-up tests help to ascertain the measures to be taken to prevent any disease.

The diagnostic care system includes services that diagnose a disease based on already existing symptoms, such as ultrasound, radiology and laboratory tests.

Regulatory Regimes Applicable to Preventative and Diagnostic Healthcare

India does not have a specific law on preventative or diagnostic health check-ups. The existing Indian laws also do not describe the terms "preventive healthcare" or "diagnostic healthcare".

However, the following regulations contain provisions relating to preventive and diagnostic healthcare in India.

- The Occupational Safety, Health and Working Conditions Code 2020 mandates every employer to provide an annual health examination or free tests to employees in specific types of work, such as factories, mines, construction work, dock work, cigar manufacturers and any other establishments prescribed by the government. The code also mandates employers to conduct free medical examinations and investigations to detect occupational diseases.
- The Income Tax Act 1961 allows individuals to claim the benefit of tax deductions on the health insurance premium, including on Preventative Health Check-ups.
- The Telemedicine Guidelines 2020 prescribe rules on healthcare services provided for diagnosis, treatment and prevention of disease and injuries using telecommunications and digital communication technologies.
- In 2015, the Indian government established the Free Diagnosis Service Initiative directing States to:
  - (a) ensure availability of a minimum set of diagnostics;
  - (b) reduce high expenditure on diagnostics;
  - (c) enable initiation and continuation of appropriate treatment based on accurate diagnosis and use of appropriate diagnostics to screen patients; and
  - (d) improve the quality of healthcare and patients' experience.
- The Indian government has also launched a few initiatives to promote preventative healthcare, such as "Ayushman Bharat: Focus on Preventive and Promotive Health", the "Fit India Movement" and "Eat Right India".

(a) The Ayushman Bharat guidelines, launched in 2018, are a framework for health and wellness centres to provide healthcare services. The guidelines require these centres to have the capacity to provide basic diagnostics and screening capacities and are in accordance with Free Diagnosis Service Initiative.
(b) The Fit India Movement was launched in 2019 to promote fitness. The Fit India mobile app was released under this initiative to track fitness levels, steps, sleep and calorie intake, as well as offering diet plans.
(c) The Eat Right India Initiative was launched in 2019 to ensure the availability of safe and wholesome food for people in India.

- The Insurance Regulatory and Development Authority of India issued Guidelines on Wellness and Preventative Benefits in September 2020 which are applicable to all life, general and health insurance companies. These guidelines suggest that insurance companies include wellness provisions in their policies, such as discounts on health check-ups, diagnostics, vouchers for memberships in yoga centres, gyms, sports club and fitness centres.
- The Indian healthcare system is slowly moving from a treatment approach to a preventative care approach. The COVID-19 pandemic led to shortage of hospital beds, oxygen, and doctors, which led the healthcare industry to realise the importance of preventative care. The pandemic enabled people to access technology including wearable gadgets, online platforms, home-based test kits, etc, to monitor their health status.

4.2 Increased Preventative Healthcare

The following factors have resulted in the increased use of preventative healthcare in India.

- COVID-19 pandemic: the pandemic was a wake-up call for people to get their health under control. The pandemic led to a high death rate across the country due to shortage of hospital beds, oxygen and doctors. This pushed people to take preventative measures at home, such as adopting healthy eating habits to build their immune system and periodically tracking and monitoring their health using wearable and medical devices such as oximeters, blood pressure monitors, blood glucose monitors and nebulisers.
- Telemedicine and telehealth: the adoption and increase in teleconsultation services in India has led to an increase in preventative healthcare. As people could not physically visit health practitioners during the pandemic, they availed themselves of remote consultations on preventative measures with the help of video/audio calls and text messages. Telehealth proved to be a cost-effective and faster way to use preventative measures. The country also experienced a tremendous increase in telecounselling services for patients suffering from mental health issues. An increase in online/live fitness (yoga or workout) programmes and platforms have also helped people to control their health and fitness from the comfort of their home.
- Government initiatives: as stated previously, the Government of India has launched a few initiatives to promote preventive healthcare, such as “Ayushman Bharat: Focus on Preventive and Promotive Health”, the “Fit India Movement” and “Eat Right India” (see **4.1. Preventative Versus Diagnostic Health**).
- Social trends: social media influencers have increased the awareness of preventative

measures and have played a great role in encouraging people to adopt healthy lifestyles and regular fitness regimes.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the Privacy Rules) describe physical, physiological and mental health conditions, medical records and medical history as "sensitive personal data or information".

The terms "fitness and wellness information" are not separately regulated or defined under Indian law.

Broadly, any information relating to a medical health condition is categorised as sensitive personal data and is currently regulated by the Privacy Rules.

As explained in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**, the Privacy Rules prescribe mandatory principles for handling and processing sensitive personal data by the body corporates handling such information. There is no separate law in India to regulate health data. The DISH Bill proposes to regulate privacy and security measures for health-related data. The Health Digital Management Policy issued by the MoHFW also lays down principles for health data protection. The DISH Bill and the Health Digital Management Policy are mainly based on the principles of the Privacy Rules.

The right to privacy of all citizens is a part of the fundamental right to life and personal liberty under Articles 19 and 21 of the Constitution of India. The Supreme Court of India has recognised the right to privacy as a fundamental right in the landmark judgment of Justice K S Puttaswamy (Rtd) and Another v Union of India and Others (2017) 10 SCC 1.

Pursuant to the aforementioned judgment, the Ministry of Electronics and Information Technology formed the Justice BN Srikrishna Committee, which introduced the Draft Personal Data Protection Bill 2019 in the lower house of the Indian Parliament (the Lok Sabha) on 11 December 2019. After consulting various stakeholders, including government agencies, regulatory bodies, companies, law firms and academics experts, the Ministry of Electronics and Information Technology introduced a revised Digital Personal Data Protection Bill 2022 (PDP Bill) in November 2022. Once enacted, the PDP Bill will become a comprehensive data protection law in India. The revised PDP Bill introduced the concept of deemed consent, the right to nominate as a data subject, omission of data localisation, the penalty for non-compliance of up to 500 crores, etc.

Currently, the Privacy Rules provide the security practices and procedures that a body corporate or any person collecting, receiving, possessing, storing, dealing or handling information on behalf of the body corporate is required to observe for protecting personal data of users.

4.4 Regulatory Developments

The MoHFW released the draft Public Health (Prevention, Control and Management of Epidemics, Bioterrorism and Disasters) Act in 2017. The MoHFW is in the process of finalising the provisions of the bill and it is expected to be introduced in Parliament this year. This bill will replace the existing Epidemic Disease Act 1897, which was implemented to control the bubonic

plague. There have been no amendments or regulations made under the Epidemic Disease Act since its implementation.

The Bill empowers central, state, district and local authorities to adopt several procedures to control the spread of epidemic-prone diseases. The Bill empowers the states to conduct medical examinations as well as provide treatment to persons suffering from such diseases.

Further, as explained in **4.1 Preventative Versus Diagnostic Healthcare**, the Occupational Safety, Health and Working Conditions Code, Income Tax, Telemedicine Guidelines, Guidelines on Wellness and Preventive Benefits and various government initiatives currently address preventative healthcare in India.

4.5 Challenges Created by the Role of Non-healthcare Companies

In recent years, several technology companies in India have developed solutions to issues in the healthcare industry, such as the following:

- Qure.ai provides AI products to healthcare professionals to conduct preventative screenings, early detection, emergency care, and treatment adherence, etc;
- Niramai Health Analytix has developed an AI-based sensing device to detect breast cancer;
- HealthifyMe provides AI-based virtual assistance, which helps users to track calorie intake and answer queries relating to fitness and nutrition;
- Artelus has developed an AI-based diabetic retinopathy screening system; and
- Tricog has developed products that interpret and analyse ECG reports and echocardiograms.

The main challenge presented by these companies relates to data protection and patient privacy. Although the Privacy Rules are applicable to health data, the increase in these new technologies in India requires a robust and comprehensive data protection regime.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

The internet of medical things (IoMT) has completely transformed the healthcare sector in India and enabled healthcare practitioners to connect faster with patients, even in remote areas, and to deliver better services. Further, the use of internet and mobile devices has increased exponentially in India and connectivity is widely available, even in the majority of rural areas.

Technologies such as AI, telemedicine, augmented and virtual reality, wearable devices (smart watches and fitness bands) have changed the landscape of the healthcare system in India. IoMT is being significantly used in India for tracking health and symptoms, treatment of disease, telemonitoring patient's health conditions, tracking medicine dosage, etc.

The COVID-19 pandemic has led to an increase in the need for remote patient monitoring and consultation and a reduction in hospital visits. This has been greatly assisted by the IoMT.

There has been an increase in demand for homecare facilities following discharge from hospital. Many healthcare service providers and hospitals in India now provide an intensive care unit system that can be set up at home. The system

includes electronic medical records, audio visuals, a smart alert system, response tools, 24-7 monitoring and assessment systems.

5.2 Legal Implications

A healthcare practitioner or a hospital can be held liable for medical negligence in cases of an adverse healthcare outcome. In this regard, there are both civil and criminal liabilities for medical negligence in India.

As regards civil liability, a complaint can be filed in the Consumer Court against the hospital (if the doctor is an employee of a hospital) or a doctor or a healthcare practitioner under the Consumer Protection Act 2019 (CP Act), claiming compensation for damages suffered by the consumer. The CPA defines the term "deficiency" as "any fault, imperfection, shortcoming or inadequacy in the quality, nature and manner of performance which is required to be maintained by or under any law for the time being in force or has been undertaken to be performed by a person in pursuance of a contract or otherwise in relation to any service and includes any act of negligence or omission or commission by such person which causes loss or injury to the consumer."

As regards criminal liability, medical negligence is treated as an offence under the Indian Penal Code 1860 (IPC). The IPC prescribes that if a person commits a rash or negligent act due to which human life or personal safety of others is threatened, such act is punishable by a maximum two-year prison term or a maximum fine of INR1,000 (USD15 approximately), or both.

Health practitioners or hospitals have the following defences:

- anything which occurs because of an accident or misfortune and without criminal intention or knowledge in the doing of a lawful act in a lawful manner by lawful means and with proper care and caution is not an offence;
- anything done that is likely to cause harm, but without any intention to cause harm and in good faith to avoid other damages to a person;
- anything done in good faith for the good of other people and does not intend to cause harm even if there is a risk involved and the patient has given implicit or explicit consent.

There are various case laws where the Supreme Court of India has granted compensation to patients in cases of medical negligence.

The Supreme Court has also recognised the Bolam Test in Jacob Mathew v State of Punjab (2005) 6 SCC 1 as a standard of ascertaining whether the act of a person would be an act of an ordinary competent person exercising ordinary skill in that profession.

In the recent case of Harish Kumar Khurana v Joginder Singh (2021 SCC SC 673), the Supreme Court observed that every death of a patient cannot, on the face of it, be considered as death due to medical negligence, unless there is material on record to that effect.

In every case where the treatment is not successful or the patient dies during surgery, it cannot be automatically assumed that the medical professional was negligent. The Court further observed that the principle of res ipsa loquitur is only applicable where the negligence is obvious. Mere legal principles and a general standard of assessment are not sufficient in case in question as there was no clear medical evidence that the patient's condition could not withstand the surgery.

5.3 Cybersecurity and Data Protection

The IoMT collects and shares a high amount of medical data of users with health practitioners, which makes it vulnerable to misuse. The patient's medical information is considered sensitive personal data under the Privacy Rules.

The contracts and healthcare institution policies are governed by the following currently applicable laws in India:

- the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (IMCR) imposes patient confidentiality obligations on medical practitioners; and
- the principles embedded in the Privacy Rules, such as:
  (a) the patient's consent before collection, storage, transfer or processing of health data;
  (b) the body corporate/healthcare institution must have a privacy policy in place as per the Privacy Rules; and
  (c) implementation of reasonable security practices and procedures for protecting the patient's health data.

The principles of Privacy Rules and privacy policy are explained in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**.

5.4 Proposed Regulatory Developments

The MoHFW introduced the DISH Bill in 2017 to regulate the generation, collection, storage, transmission, access and use of all digital health data. The DISH Bill also provides for the establishment of a National Digital Health Authority as a statutory body to enforce privacy and security measures for health data and to regulate the storage and exchange of health records. The principles in the DISH Bill are based on the PDP Bill. However, the DISH Bill does not specifically define "internet of medical things" or "internet of things".

The MoHFW has also approved a Health Data Management Policy based on the PDP Bill to govern data in the National Digital Health Ecosystem. The Health Data Management Policy also does not specifically define internet of medical things or internet of things; however, the policy is applicable to all methods of contact, including via internet or email.

The provisions of the DISH Bill and Health Data Management Policy are explained in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

The MoHFW introduced the DISH Bill in 2017 to regulate the generation, collection, storage, transmission, access and use of all digital health data. The DISH Bill also provides for the establishment of a National Digital Health Authority as a statutory body to enforce privacy and security measures for health data and to regulate the storage and exchange of health records. The principles in the DISH Bill are based on the PDP Bill. However, the DISH Bill does not specifically define "internet of medical things" or "internet of things".

The MoHFW has also approved a Health Data Management Policy based on the PDP Bill to govern data in the National Digital Health Ecosystem. The Health Data Management Policy also does not specifically define internet of

medical things or internet of things, however, the policy is applicable to all methods of contact, including via internet or email.

The provisions of the DISH Bill and Health Data Management Policy are explained in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**.

The MoHFW issued a notification on 11 February 2020 (the "MoHFW Notification") specifying that medical devices be treated as drugs with effect from 1 April 2020. Therefore, all the regulations and compliances applicable to drugs are also applicable to medical devices. The MoHFW Notification stipulates that a medical device is an instrument, apparatus, appliance, implant, material or other article, including a software or an accessory for the purposes of:

- diagnosis, prevention, monitoring, treatment or alleviation of any disease or disorder;
- diagnosis, monitoring, treatment, alleviation or assistance for any injury or disability;
- investigation, replacement or modification or support of the anatomy or of a physiological process;
- supporting or sustaining life;
- disinfection of medical devices; and
- control of conception.

The DCGI is responsible for the administration and approval of manufacturing, importing or marketing of medicinal products and medical devices in India. As a medical device now includes software, the DCGI is also responsible for software as a medical device. The D&C Act and the Drugs and Cosmetics Rules 1945 (DCR Rules), and the Medical Devices Rules 2017 (MDR) govern approvals and define whether a product is categorised as a drug or any other category.

The CDSCO classifies medical devices into four main categories, based on the risk of use.

However, currently, there are no specific regulatory frameworks or guidelines to categorise or classify software as a medical device in India. Therefore, it is difficult to ascertain which computer software/mobile application qualifies to be a medical device. This is a challenge common to application service providers, developers and stakeholders in India.

Similarly, there is no clarity on whether the Prices Control Order, which is applicable to drugs, will also apply to medical software applications and whether they will be able to control the price of their digital health-related software products.

Also, there is currently no specific legal framework in India for software based on AI and machine learning.

It is the common consensus of stakeholders in India that the government should adopt effective regulatory frameworks based on risk of use, and AI/machine learning, similar to the International Medical Device Regulation Forum's medical software device framework and the US FDA's Artificial Intelligence and Machine Learning Software as a Medical Device Action Plan.

7. Telehealth

7.1 Role of Telehealth in Healthcare

India uses the New England Journal of Medicine (NEJM) Catalyst definition of "telehealth", namely the delivery and facilitation of health and health-related services including medical care, provider and patient education, health information services, and selfcare via telecommunications and digital communication technologies.

Telehealth is a broad term used for technology for health and health-related services, including telemedicine.

Telehealth is a solution for providing timely and faster access to medical treatment. It also reduces the costs and efforts associated with travel to receive medical treatment, especially for people in rural India. The telecommunication technologies can also maintain patients' medical records and can help patients manage their medication and diseases better. Telehealth has proven to be very beneficial in India, especially during the COVID-19 pandemic.

There have been various efforts made to promote telehealth in India. The India Virtual Hospital, a medical technology service in India, launched the Patient Care App, which enables doctors to track a patient's health and recovery. Another health-tech company has recently launched an online platform, iCliniq, where users can get medical advice from doctors/medical practitioners, physicians and therapists from the USA, the UK, UAE, India, Singapore, Germany, and other countries, using emails, online chats and video and audio calls. Another Indian company set up a virtual hospital for cancer patients in 2019 for online consultation, treatment planning, and cancer treatment management.

7.2 Regulatory Environment

India currently does not have specific legislation that regulates telehealth or the use of online platforms in respect of telehealth.

As a result of the COVID-19 pandemic, the Indian government issued the Telemedicine Practice Guidelines (TPG) which are intended to enhance healthcare services and enable access to all. The guidelines are meant for registered medical practitioners, and prescribe the norms and standards for consulting patients, including all channels of communication with the patient that leverage IT platforms, including voice, audio, text and digital data exchange.

The TPG specifically exclude specifications for hardware or software, infrastructure building and maintenance, data management systems, standards and interoperability or the use of digital technology to conduct surgical or invasive procedures remotely. Other aspects of telehealth, such as research and evaluation and the continuing education of healthcare workers and consultations outside the jurisdiction of India, are also included in the guidelines.

The TPG mandates a registered medical practitioner to obtain consent from the patient before a telemedicine consultation. If the patient voluntarily initiates the telemedicine consultation, the consent is implied.

The principles regarding medical ethics, data privacy and confidentiality apply to the registered medical practitioners.

7.3 Payment and Reimbursement

The TPG prescribes that the telemedicine consultations must be treated the same way as in-person consultations, from a fee perspective. The registered medical practitioner must also provide a receipt/invoice for the fee charged for the telemedicine consultation.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

The internet of medical things (IoMT) includes digital medical devices and software applica-

tions used to provide effective and efficient services to patients and to reduce the cost of healthcare. Recent technologies, such as sensors, wearable devices, health apps, telemedicine, AI, oxygen and heart monitors, are widely used in India. The IoMT technologies make it easier for doctors and medical practitioners to track the progress of treatment and recovery in real time.

In the wake of the COVID-19 pandemic, the medical establishment began urging people to adopt the IoMT for teleconsultations, remote monitoring and treatment, thereby eliminating hospital visits. The Indian government has encouraged hospitals to adopt electronic health records containing patients' health history and records.

An increase in IoMT technologies also brings an increase in the data privacy risks and related issues because of the lack of adequate and specific regulations, a lack of awareness among the users and the service providers' lack of compliance in the absence of a comprehensive legal framework in the country.

Technological issues, such as the compatibility of hardware and software with cloud services, are also a factor to be taken into consideration.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

5G networks were launched in India in 2022. The higher speed and connectivity and low latency in the 5G network have boosted advanced telehealth solutions and improved the healthcare system in India. 5G networks ensure more effectiveness and efficiency in teleconsultations and remote monitoring of patients as well as the handling of patients' health data.

5G networks are also helpful in the country's rural areas, which lack adequate telecommunication infrastructure, through the following:

- faster transmission of large health data files;
- high-quality video/audio telecommunications between doctors and patients;
- improved use of augmented and virtual reality; and
- enhanced use of AI in healthcare devices.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

Information relating to a person's health is categorised as sensitive personal information under the Privacy Rules. The Privacy Rules lay down mandatory principles of data privacy to be followed by the body corporates that handle and process sensitive personal information.

The primary requirement for body corporates under the Privacy Rules is to obtain written consent from the information provider before collecting and processing the sensitive personal data. Prior consent is also required for sharing sensitive personal data with third parties.

The information provider must be informed of the fact that sensitive personal data is being collected, the intended purpose of its use and whether it will be transferred to any third parties, along with the contact details of the agency collecting the information. It is also mandatory under the Privacy Rules for the body corporates to have a privacy policy containing the type of sensitive

personal information collected, the purpose of collection, disclosure of that information, and the reasonable security practices and procedures to be implemented by the body corporates. India does not yet have a comprehensive data protection law. However, the government has issued the PDP Bill, which is intended to become a comprehensive data protection law in the country.

There is no separate legislation in India regulating data privacy issues for digital health. However, the proposed DISH Bill aims to address the data privacy issues relating to digital health, and is primarily based on the principles laid down under the PDP Bill. The MoHFW has also issued the Health Data Management Policy, which outlines the principles for the protection of an individual's personal digital health data privacy.

The DISH Bill proposes that a clinical establishment may, by duly obtaining written consent (on paper or electronically) from the owner, lawfully collect the required health data after informing the owner of the data of the following:

- the rights of the owner, including the right to refuse to give consent to the generation and collection of their data;
- the purpose of the collection of their health data;
- identity of the recipients to whom the health data may be transmitted or disclosed, after being converted into a digital format; and
- the identity of the recipients who may have access to that digital health data, on a need-to-know basis.

Further, the clinical establishment or any other entity must furnish a copy of the consent form to the owner of the data.

The current regulations do not specifically regulate the sharing of personal health data by a wearable healthcare device.

The Privacy Rules do not prescribe de-identification or anonymisation of data. However, the DISH Bill and Health Data Management Policy defines "anonymisation" as the process of permanently deleting all personally identifiable information from an individual's digital health data. "De-identification" is defined as the process of removing, obscuring, redacting or de-linking all personally identifiable information from an individual's digital health data in a manner that eliminates the risk of unintended disclosure of the identity of the owner and that, if necessary, makes it possible for the data to be linked to the owner again.

The DISH Bill proposes that de-identified or anonymised data must be used only for the following purposes:

- improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bio-terror events and infectious disease outbreaks;
- facilitate health and clinical research and healthcare quality;
- promote the early detection, prevention, and management of chronic diseases;
- carry out public-health research, review and analysis, and policy formulation; and
- undertake academic research and other related purposes.

The Health Data Management Policy prescribes that data fiduciaries may make anonymised or de-identified data in an aggregated form available for the following purposes:

- facilitating health and clinical research, academic research;
- archiving;
- statistical analysis;
- policy formulation;
- the development and promotion of diagnostic solutions; and
- any other purposes that may be specified by the National Digital Health Mission (NDHM).

The NDHM must set out a procedure through which any entity seeking access to anonymised or de-identified data will be required to provide relevant information, such as its name, purpose of use and nodal person of contact. Subject to approval being granted under this procedure, the anonymised or de-identified data must be made available to that entity on whatever terms may be stipulated on its behalf.

Any entity provided access to de-identified or anonymised data must not, knowingly or unknowingly, take any action that has the effect of re-identifying any data principal or the effect of any such data no longer remaining anonymised.

The data fiduciary that is undertaking to anonymise or de-identify data must be responsible for ensuring compliance with the procedure for the anonymisation or de-identification as set out by the NDHM. The de-identification or anonymisation of data by a data fiduciary must be done in accordance with technical processes and anonymisation protocols that may be specified by the NDHM. The technical processes and anonymisation protocols must be periodically reviewed by the NDHM.

The Information Technology Act 2000 prescribes that a body corporate, possessing sensitive personal data that is negligent in implementing and maintaining reasonable security practices and procedures, will be liable to pay damages by way of compensation. It also prescribes that if a body corporate has obtained sensitive personal data without the consent of the information provider, and discloses the information to any other person, this is punishable by a maximum two-year prison term or a maximum fine of INR100,000 (approximately USD1,400), or both.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

New technologies are emerging in the digital health sector in India, including AI and machine learning. Currently, India does not have any legislation to regulate technologies such as AI/machine learning. However, the TPG prescribes that the telemedicine platforms based on AI/machine learning are not permitted to counsel patients or prescribe any medicines to a patient. The technologies such as AI, the Internet of Things and advanced data science-based decision support systems may be used only to assist and support the clinical decisions of a registered medical practitioner. In all cases, the final prescription or counselling must be delivered directly by a registered medical practitioner.

With the growth of AI technologies in India, the Indian government authorised the public policy think tank, the National Institution for Transforming India Commission (NITI Aayog) to address strategy on AI-based technologies/machine learning in the agriculture and health sectors. In June 2018, the NITI Aayog issued a discussion paper on national strategy for artificial intelligence for healthcare, agriculture, education, smart cities and infrastructure and smart mobility and transportation. The discussion paper recognised AI, combined with robotics and IoMT,

as the new nervous system for healthcare in India, presenting solutions to address healthcare problems. Currently, the NITI Aayog is reportedly working with a large Indian hospital, the Tata Memorial Centre, to launch a digital pathology and imaging bio-bank for cancer detection.

AI/machine-learning technologies use and share medical conditions of patients with doctors/medical institutions, which is considered as sensitive personal data under the Privacy Rules. The Privacy Rules prescribe mandatory compliance with the principles of data protection by body corporates that handle, store and process sensitive personal data.

In February 2021, the NITI Aayog issued principles for the responsible use of AI. The NITI Aayog stated that the AI solutions must comply with the principles of data protection laid down in the PDP Bill, such as consent, purpose limitation and rights to the information provider. AI solutions must maintain the privacy and security of medical information/data, which is sensitive personal data, and ensure sufficient safeguards.

Electronic health records (EHR) can ensure the easy accessibility of a patient's records from anywhere at any time, easy storage, and can help in tracking the patient's progress. The DISH Bill and Health Data Management Policy also promote EHRs. The Indian government issued recommendations in 2016 on different standards for different purposes in respect of EHRs. For example, ISO/TS 22220:2011 Health Informatics – Identification of Subjects of Health Care, must be complied with to obtain basic identity details of patient; ISO/TS 14441:2013 Health Informatics – Security & Privacy Requirements of EHR Systems for Use in Conformity Assessment must be complied with to maintain basic data security and privacy requirements, and ISO TS 14265:2011 is for the processing of personal health information.

The 2016 EHR standards recommendations stipulate that only those persons, including organisations, duly authorised by the patient may view the recorded data or part thereof. The term "security" refers to all recorded personally identifiable data, which will at all times be protected from any unauthorised access, particularly during transport (eg, from healthcare provider to provider, healthcare provider to patient). The term "trust" refers to that person, persons or organisations (doctors, hospitals, and patients). The 2016 EHR standards recommendations are based on the principles of data protection laid down under the Privacy Rules.

The Ayush Grid Project

The Ayush Grid Project is developed by the Ministry of Ayush with the aim of creating a comprehensive information technology backbone for the health sector, which envisages digitisation of service delivery across the six functional areas – health services, education, research, drug administration, and medicinal plants.

11.2 AI and Machine Learning Data Under Privacy Regulations

Currently, there are no proposed or enacted regulations in India that address the use of AI and machine learning data in healthcare.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Companies developing healthcare technologies in India are operating without a specific legislation on digital healthcare and, as a result, many general laws are applicable to such companies,

such as the Privacy Rules, CPA, IPC, etc. The healthcare providers must have a privacy policy under the Privacy Rules for collection, storage, processing and transfer of health data (ie, sensitive personal data). The Privacy Rules prescribe additional compliances for such digital healthcare providers, especially if they qualify as an intermediary under the Information Technology Act 2000 (IT Act).

Digital healthcare companies collect huge amounts of sensitive personal data from users; therefore they must adopt reasonable security practices and policies to adhere to the Privacy Rules.

In the absence of specific legal provisions governing digital healthcare using virtual assistance and AI, companies using such technologies must comply with the Privacy Rules as well as the TPG.

Further, digital healthcare service providers are required to ensure that a user's medical prescription is not automatically generated, but each prescription must be thoroughly verified and expressly endorsed by a registered medical practitioner. However, in the absence of a specific legal guidance, the service providers will have to comply with requirements under multiple legislations and regulations.

The D&C Rules mandate that every prescription must be in writing and signed by the registered medical practitioner. However, online service providers are finding it difficult to generate such prescriptions with the practitioner's signature and companies are now looking to generate prescriptions using the practitioner's digital signature to be considered as valid under the IT Act provisions. The Delivery Notification issued by the MoHFW also allows medicines to be delivered based on receipt of a prescription physically or by email.

Similarly, there is no specific law to regulate e-pharmacies in India. Currently, e-pharmacies are required to comply with the licence requirements and online prescription requirements under the D&C Act as well as the IT Act. The MoHFW has issued Draft E-Pharmacy Rules, 2018 ("draft rules") to regulate e-pharmacies under the D&C Act, which are yet to be enacted. Additionally, e-pharmacies are also required to comply with the Delivery Notification.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

India is developing and adopting various technologies in the fields of telehealth, AI/machine learning and the IoT in order to adopt the digital healthcare system. The IT infrastructure must be able to manage and secure the large amount of health data collected by the devices. Besides this, India requires a comprehensive data privacy and protection law to address the privacy and security risks related to digital health data.

13.2 Data Management and Regulatory Impact

Currently, there are no proposed or enacted regulations in India on the implementation of IT upgrades.

14. Intellectual Property

14.1 Scope of Protection

The digital healthcare system thrives on novel ideas, inventions, and advancements in software applications and smart devices. Indian intellectual property laws allow for the protection of pat-

ents, copyrights, trade marks and designs. From the digital health standpoint, the key areas of development are in the area of software.

Patents Act 1970 (Patents Act)

In India, patents are examined, granted and administered by the Patents Act, which complies with the Trade-Related Aspects of Intellectual Property Rights agreement. India is also a signatory to the Paris Convention, in addition to the Patent Co-operation Treaty. A digital health mechanism is essentially a software/computer program. Although the Patents Act excludes protection for standalone computer programs (Section 3(k) of the Patents Act), a piece of software claimed in conjunction with a novel hardware element will be patentable in India (Guidelines for Examination of Computer-Related Inventions 2017). Further, the Delhi High Court recently held that a computer program that demonstrates a technical effect or a technical contribution will be patentable in India. Software patents are subject to other restrictions under the Patents Act, including Section 3(i) of the Patents Act, which excludes patent protection for any process for medicinal, surgical, curative or other treatment of human beings or animals.

The Patent Office has granted several patents for software programs that involve hardware elements. Therefore, digital health mechanisms, including computer software/programs embedded in mobile software applications, wearable devices, etc, may be protected in India, as long as they include a novel hardware element.

Copyright Act 1957 (CRA)

The CRA provides for copyright protection in India. The CRA provides that a copyright subsists in the form of original literary, dramatic, musical or artistic work, cinematographic films and sound recordings. Although copyright registration is not mandatory for protection in India, a copyright registration will serve as evidence of the copyright in the work. The CRA covers computer programs under the purview of literary work, therefore, the literary portions of a computer program, including the source code, are protected under the CRA.

Trade Marks Act 1999 (TM Act)

The TM Act provides for trade mark protection in India. The TM Act not only accords statutory protection for registered trade marks, but also recognises common law protection to unregistered trade marks in India. Trade mark protection in India extends to any device, brand, label, word, shape of goods, packaging or, combination of colours or any combinations thereof. Under Indian law, digital healthcare providers can claim trade mark protection for their brand names, logos, labels, names of devices/software applications, shape of medical goods or wearable devices, packaging, etc.

Designs Act 2000 (Designs Act)

The Designs Act provides for protection of industrial designs in India, and it extends to features of shapes, configurations, patterns, ornaments or composition of lines, or colours that are applied to an article. From the digital health standpoint, the key areas where design protection can avail are with respect to graphical user interface of software applications, mobile applications, or similar computer programs used on medical devices, screen layout of a program, etc, so long as they do not fall within the exceptions under the Designs Act.

Trade Secrets

Currently, there is no legislation or statutory protection for trade secrets in India. However, different courts in India have extended protection for trade secrets and confidential information,

provided that the information's confidentiality is reflected in contractual documents, such as Confidentiality Agreements, Non-Disclosure Agreements, and reasonable and legally enforceable non-compete clauses in the agreements.

There is no specific legislation or statutory protection for databases in India, nor in respect of data and databases used in machine learning. However, the CRA provides protection to a computer database under the purview of literary work. The CRA also provides protection for databases by granting rights associated with the labour involved in compiling and presenting data in a particular form.

14.2 Advantages and Disadvantages of Protections

Patent Protection

The grant of patent enables the patent owner to prevent others from infringing the invention (ie, manufacturing or selling the invention without the owner's consent). The protection enables the owner to enjoy a monopoly over the invention and to license the patent to a third party and gain profits. The patent grant also allows owners to publicly disclose their invention, potentially attracting investors, stakeholders, and consumers.

One of the key challenges faced by patent applicants in India is the lack of straightforward, broad protection for software patents. A digital health mechanism is essentially a software in the form of a computer program or a mobile software application. The Patents Act excludes protection for standalone computer programs (Section 3(k) of the Patents Act), unless the protection for such a program is claimed in conjunction with a novel hardware element. Further, software patents are also subject to other restrictions under the Patents Act, including Section 3(i) of the Patents Act, which excludes patent protection for any process for medicinal, surgical, curative or other treatment of human beings or animals.

Additionally, while the term of a trade mark can be extended indefinitely by renewing the registration every ten years, patent protection in India is only valid for 20 years.

Also, patent protection can be expensive for companies as the official fees for filing and periodic maintenance of the patents can run into several thousands of dollars, especially if the applicants choose to protect their inventions in other jurisdictions. Further, initiating a patent infringement suit and defending a patent in Indian courts may also involve significant costs. However, the 2016 amendment to the Patents Rules 2003 offers heavily discounted fees for start-up companies and small enterprises.

Finally, there is a significant backlog in many departments of the Patent Office's examination section. However, patent applicants can engage qualified local attorneys who can help expedite the patent prosecution by taking measures, such as carrying out proper freedom to operate searches, understanding the filing requirements beforehand, thereby avoiding objections and consequent delays at the examination stage. An attorney's personal rapport with the Patent Office officials may also help in understanding the nature of objections and resolving them in a timely manner.

The timeframes of patent prosecution are gradually shortening as a result of modernisation of patent offices and an increase in the number of examiners.

Copyright Protection

Copyright protection prevents losses arising from piracy. Although copyright registration is not mandatory in India, copyright registration makes it easier to prove copyright ownership in courts.

Trade Mark Protection

One of the key advantages of trade mark protection in India is that the proprietors can continue to extend the life of trade marks indefinitely by renewing the protection every ten years. Moreover, the recent amendments to the Trade Marks Rules 2003 have introduced discounted official fees applicable to start-up companies and small enterprises.

The Indian Courts fully recognise the rights of patent owners and grant protection in infringement matters. In the case of Indoco Remedies Ltd v Bristol Myers Squibb Holdings, 2020 (83) PTC 551 (Del), the Delhi High Court prohibited Indoco from selling the drug "APIXABID", as Bristol is a patent owner of the drug "APIXABAN" for treating COVID-19 and which was easily available to consumers.

In the case of Microsoft Corporation and Another v Kanhaiya Singh and Another, 5 W.P.(CRL) 558/2016, the Delhi High Court directed the defendant to pay compensation for damages and prohibited them from software piracy and passing off Microsoft's software. There is also much leading case law in India on various issues of trade mark infringement and passing off, allowing the owners to claim proprietary rights over their trade marks in exclusion of others.

14.3 Licensing Structures

There are multiple types of licensing arrangements used in India, which are applicable to digital healthcare, such as software, patent, copyright and technology licensing.

Broadly, there are three types of intellectual property licensing arrangements used in India:

- exclusive licensing, whereby only the licensee is authorised to use the intellectual property;
- non-exclusive licensing, allowing one party to license the intellectual property to more than one licensee; and
- sole licensing, whereby only the licensor and licensee may use the intellectual property.

14.4 Research in Academic Institutions

The ownership of IP in India varies under different IP laws. With regard to copyright, the employer (university or healthcare institution) will be the first owner of the copyright, not the physician or the inventor. However, this will not apply in the case of an independent contractor-developed copyright. Regarding the patents, the inventor will be the first owner, irrespective of whether they are an employee or a contractor.

14.5 Contracts and Collaborative Developments

In India, the institutions or universities or employers enter into development agreements with their employees. Standard development agreements normally provide that all the IP developed by the employees/inventors/researchers under the agreement will be assigned to and owned by the employers.

15. Liability

15.1 Patient Care

The TPG prescribes that the platforms based on AI/machine learning are not permitted to counsel or prescribe any medicines to a patient.

However, technologies such as AI, the IoT and advanced data science-based decision support systems may be used only to assist and support the clinical decisions of a registered medical practitioner. In all cases, the final prescription or counselling has to be delivered directly by the registered medical practitioner. Therefore, the liability falls on the doctors or other medical service providers. Consumers can claim compensation from doctors/hospitals under the CP Act. Criminal liability can be imposed on the doctors, on grounds such as:

- causing death by negligence;
- endangering the life or personal safety of others;
- causing hurt by an act endangering the life or personal safety of others; and
- causing grievous hurt by an act endangering the life or personal safety of others.

15.2 Commercial

Third parties supplying products and services to healthcare institutions can be subject to civil and criminal liabilities, penalties and actions under the CP Act. They can also be held liable for penalties prescribed under the IT Act for data breaches.

Trends and Developments

Contributed by:
Anoop Narayanan and Sri Krishna
ANA Law Group

ANA Law Group is a full-service law firm based in Mumbai. Its team of experienced and committed professionals has broad industry knowledge and specialises in a wide spectrum of the law. Founded on traditional values and with prominent cross-border exposure, the firm has significant experience in counselling international clients on data protection and privacy in India, acting for many businesses in complex transactions. ANA Law Group has in-depth knowledge of all sectors of industry, such as banking and insurance, financial institutions, luxury goods, consumer goods and healthcare. The firm assists international companies on global privacy law involving Indian projects, drafting and negotiating contracts with their Indian counterparts, preparing data protection and privacy policies for those companies' Indian subsidiaries, compliant with major international privacy laws. Specifically, the firm advises clients on data processing and all aspects of data security, including handling cross-border data flows, security breaches and compliance with all regulatory requirements.

Authors

Anoop Narayanan is the founder of ANA Law Group and a leading Indian lawyer in corporate law, intellectual property law and information technology with three decades of experience as an attorney. Focusing on a broad range of intellectual property, IT, outsourcing, employment, technology, data protection, telecommunications and entertainment law matters, his practice encompasses both litigation and commercial or transactional advice. He has worked with India's highest-profile companies, as well as global corporates in the manufacturing, banking and finance sectors and telecommunications and technology companies. His experience and expertise in TMT and data privacy was invaluable in setting up the Indian operations of large global technology companies and handling several India-bound outsourcing transactions with the major Indian IT companies.

Sri Krishna is an associate at ANA Law Group working in its TMT and IP practice group. He regularly advises international clients on intellectual property, healthcare and pharmaceuticals-related issues in transactional, compliance and regulatory matters.

ANA Law Group

7th Floor, Keshava
Bandra Kurla Complex
Bandra East
Mumbai
400 051
India

Tel: +91 22 6112 8484
Fax: +91 22 6112 8485
Email: anoop@anaassociates.com
Web: www.anaassociates.com

In the three years since the outbreak of the pandemic, India has experienced a remarkable upsurge in the digitalisation of the healthcare system. This is manifested in the widespread use of technologically advanced tools for rapid testing, effective diagnoses, telemedicine, teleconsultations, and home delivery of medicines, among other applications. Telemedicine and teleconsultations, in particular, have grown in popularity, with many people opting for these digitally-driven services over traditional healthcare services.

Emerging Technologies in Digital Healthcare in India

Telemedicine

Telemedicine refers to the practice of employing various information and communication technologies to facilitate virtual healthcare, where both the patient and the healthcare provider interact remotely. This encompasses the use of tools for conducting patient consultations through video, audio, or text-based mediums. While telemedicine has been prevalent in India for quite some time, the COVID-19 pandemic triggered a significant surge in its adoption. According to a survey by Practo, a prominent Indian health-tech firm, in-person appointments saw a 32% drop while online medical consultations skyrocketed by an astounding 300% between March and November 2020.

In view of this, the Ministry of Health and Family Welfare of India (MoHFW) introduced the Telemedicine Practice Guidelines (TPG) in March 2020. The TPG were introduced to assist medical practitioners in providing effective, safe and fast medical care online. The TPG prescribe regulations relating to:

- the physician-patient relationship;
- issues of liability and negligence;
- evaluation, management and treatment;
- informed consent;
- continuity of care;
- referrals for emergency services;
- medical records;
- privacy and security of the patient records and exchange of information;
- prescribing;
- reimbursement;
- health education; and
- counselling.

The TGP are applicable to registered medical practitioners (ie, those who are enrolled in the State Medical Register or the Indian Medical Register under the erstwhile Indian Medical

Council Act 1956 and current National Medical Commission Act 2019 ("NMC Act")). Under the existing framework, the TGP do not apply to registered medical practitioners outside India.

With multiple lockdowns and movement restrictions throughout the country during the last two years, healthcare workers and doctors have been using telemedicine solutions to provide timely and faster access to patients. Telemedicine was found to be cost-effective and significantly reduced the difficulties associated with patients travelling to visit a hospital or doctor. Telecommunication technologies can also maintain patients' medical records and help patients to manage their medication and diseases better.

During the nationwide lockdown in 2020–21, as patients were forced to stay at home, healthcare practitioners started to provide remote consultations using video or audio calls and text messages. During that time, technology-based consultations were also extended to COVID-19 patients with mild symptoms where hospitalisation was not required.

In addition, many healthcare organisations and doctors have been providing online counselling for the increased number of people with mental health issues caused by COVID-19 quarantine measures. This includes non-affected people whose mental health was adversely affected by the lockdown.

Further, there were various efforts made to promote telehealth in India. The India Virtual Hospital, a medical technology service, launched the Patient Care App, which enables doctors to track patient's health and recovery periodically. Another health-tech company has recently launched an online platform, iCliniq, where users can receive medical advice from medical practitioners, physicians and therapists from the USA, UK, UAE, India, Singapore, Germany, and other countries, using email, online chat and video and audio calls. Another Indian company set up a virtual hospital for cancer patients in 2019, for online consultation and treatment planning and management.

The Indian Council of Medical Research (ICMR) approved the first self-test COVID-19 kit in May 2021, which enabled users to conduct COVID-19 tests at home and obtain results within 20 minutes through a mobile app. As at March 2022, the ICMR has approved ten such self-testing kits, including those manufactured by foreign companies, such as Roche, Abbott, and Healgen. Moreover, the ICMR has declared that the US-FDA approved antigen-based COVID-19 self-test kits are exempted from ICMR validation.

The telemedicine platforms currently governed under the NMC Act are:

- the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 ("IMC Regulations"),
- the Drugs and Cosmetics Act 1940 ("D&C Act"),
- the Drugs and Cosmetic Rules 1945 ("D&C Rules"),
- the Clinical Establishment (Registration and Regulation) Act 2010,
- the Information Technology Act 2000 ("IT Act"), and
- the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("Privacy Rules").

Further, in cases of medical negligence, an aggrieved person may lodge a complaint before the relevant consumer forum under the Consum-

er Protection Act 2019, within two years from the date of injury. Similarly, a civil suit for damages, a criminal petition under the Indian Penal Code 1860, or a complaint with the NMC can also be initiated. Currently, there is no law in India that governs online consultation provided by foreign medical practitioners.

Wearable devices

Several wearable devices are now available in India, that can track heart rates, blood oxygen levels, water consumption, weight, sleep patterns and diet. These devices allow the patients to self-detect any physiological changes in the body and alert them to possible arising issues. All medical devices are regulated by the NMC Act, IMC Regulations, the Medical Devices Rules 2017, the IT Act and the Privacy Rules. Although there are no specific rules or regulations pertaining to wearable devices, the above-mentioned Acts will apply to such devices as well. Under the current regulatory framework, medical wearable devices require registration and approval from the Central Drugs Standard Control Organisation (CDSCO) in India.

For instance, the CDSCO recently approved three medical wearable devices in India, namely the Smart Vital, Vital 3.0 and Vital EGC from GOQii, a California-based fitness company. These devices measure body temperature, pulse oximeter, heart rate, sleep, blood pressure, steps taken and exercise performed.

There has been a significant rise in the number of online pharmacies in India that deliver medicines to patients' homes in the past few years, more so during the pandemic. Although the manufacture and sale of medicines are regulated by the D&C Act, D&C Rules, Registration and Regulation Act, NMC Act and IMC regulations, there is currently no law in India that specifically governs online pharmacies. The MoHFW issued a notification in August 2018 to amend the D&C Rules to bring online pharmacies under its purview ("Draft Rules").

The Draft Rules include provisions for the sale of drugs by e-pharmacies. Further, the Draft Rules define the term "e-pharmacy" as the distribution or sale, stocking, exhibiting or offering for sale of drugs through a web portal or any other electronic means. The Draft Rules contain provisions for registration and validity of e-pharmacies; conditions for registration imposed on the e-pharmacies such as location, disclosure of information, the procedure for distribution and sale, etc. While the Draft Rules are yet to be enacted, e-pharmacies in India currently require registration with the CDSCO.

Online pharmacies will also have to adhere to the Privacy Rules in relation to collecting, handling and processing patients' sensitive personal information, including financial information, bank account details, physical, physiological and mental health data, sexual orientation, medical records and history, and biometric information.

Artificial intelligence (AI)

AI-based systems are used for disease diagnosis and also for treatment purposes. Robotic surgeries allow doctors to perform complicated procedures with the help of automated machines. AI is also used for vaccine development, thermal screening, CT scans, etc. The AI-based systems are also regulated by the NMC Act, IMC Regulations, the Medical Devices Rules, 2017, IT Act and the Privacy Rules. India is home to several globally renowned multi-speciality hospitals and centres that are equipped with highly sophisticated technologies. With the increasing role of robotic surgeries and AI in healthcare in India, the Insurance Regulatory and Develop-

ment Authority of India issued Guidelines on Standard Individual Health Insurance Product in January 2020, directing insurers to cover robotic surgeries under their standard health insurance policies.

Electronic Health Records (EHR)

Digital health data records provide easy access to patients' medical history so that doctors can have relevant consultations and make recommendations, in an efficient and timesaving manner. Digital health records also eliminate duplication of tests and significantly save costs. Many private general, multi-speciality, and super-speciality hospitals in India maintain EHR databases; however, most government hospitals have not as yet upgraded to their use.

The MoHFW enacted the Electronic Health Record Standards in 2013, and revised these standards in December 2016 by issuing the new Electronic Health Record Standards 2016 ("EHR Standards"). All EHR technologies must comply with the EHR Standards. These EHR Standards are largely based on the principles of data protection laid down under the Privacy Rules. Most recently, the Indian state of Kerala successfully deployed an efficient EHR system by collecting and storing the EHRs of over 25.8 million people as part of its e-Health project. This initiative has allowed patients to walk into any government hospital without needing to bring any paper records with them.

With the increasing demand for contactless procedures, especially since the pandemic, several state governments are in the process of adopting EHR systems and other such digital mechanisms to maintain health records.

Online aggregators for health services

There are several new online platforms in India that allow users to search for doctors with different specialities in a particular region. These platforms also allow users to book online appointments with doctors and provide reviews and ratings of these doctors. Currently, there is no specific law in India that regulates online health aggregator platforms. However, the MoHFW issued a direction in January 2021 to all state governments to regulate online health aggregator platforms. Under the existing regulatory framework, as with online pharmacies, these online health aggregator platforms will require registration with the CDSCO.

The increasing number of technologies collecting health data gives rise to concerns relating to data protection and the privacy of patients. Information relating to a person's health is categorised as sensitive personal information under the Privacy Rules. The Privacy Rules lay down mandatory principles of data privacy to be followed by the body corporates collecting, handling and processing sensitive personal information. India does not currently have a comprehensive data protection law. The Indian government introduced the Personal Data Protection Bill 2019 ("PDP Bill") in the lower house of the Indian Parliament, which was referred to a Joint Parliamentary Committee (JPC). The JPC presented a revised version of the PDP Bill in Parliament in December 2021. Once enacted, the PDP Bill will become a comprehensive data protection law in India.

There is no specific law in India that regulates digital health tools and digital health data. However, the government has taken several new initiatives to address the privacy concerns relating to digital health in India, as explained below.

Healthcare Regulatory Developments in India

The Indian government enacted the draft Digital Information Security in Healthcare Act 2018 (the "DISHA Bill") to protect the digital health data of Indian citizens. The DISHA Bill defines the term "digital health data" as an electronic record of health-related information about an individual. The government proposed the DISHA Bill to standardise and regulate the processes related to collection, storing, transmission and use of digital health data, and to ensure the reliability, data privacy, confidentiality and security of such data. However, India is yet to adopt legislation to regulate and govern digital health tools in India.

As a temporary measure, the Indian government issued the TPG in March 2020, which contain norms and standards for registered medical practitioners to consult patients via digital means. The TPG regulate all channels of communication with patients that leverage information technology platforms, including voice, audio, text, and digital data exchange.

The Indian government also issued the Health Data Management Policy in October 2020 to impose standards for data privacy protection in India. The DISHA Bill and the Health Data Management Policy are both based on the data privacy principles laid down under the PDP Bill.

In 2020, the Indian government introduced the National Digital Health Mission in India based on the Health Data Management Policy. The National Digital Health Mission was renamed "Ayushman Bharat Digital Mission" in 2021 and aims to develop an integrated digital health infrastructure in India. Under this Mission, the government has introduced the ABHA App, which allows users to store, access and share their health data with health centres and healthcare professionals who are registered with the Mission. The users are given full control over their health data. The app is also integrated with Sandbox, which will test the products and technology used by the registered health companies before rolling it out to large numbers of consumers. In April 2022, after receiving public feedback, the NHA released a Draft Health Data Retention Policy (HDR Policy) for further consultation. The HDR Policy aims to create a uniform system for governing the operation of data fiduciaries, data processors, health information providers/users and data repositories within the National Digital Health Ecosystem.

In the Union Budget 2022, the Indian government announced the release of an open platform for the National Digital Heath Ecosystem, containing digital registries of health providers and access to health facilities. The Indian government has also announced the launch of the National Telehealth Programme in 2022 to enable people of all ages to access quality mental health counselling and care services. The programme is expected to establish 23 telehealth centres for mental health in India.

The government also launched the Unified Health Interface in 2022, a digital healthcare platform that will connect healthcare service providers with patients for bookings, consultations, etc.

Other Emerging Trends and Developments in India

The rise in digital solutions

Besides the use of telemedicine/telehealth in the Indian healthcare sector, there was a rapid increase in digital payments during the COVID-19 pandemic. People of all age groups have become accustomed to carrying out digital payments to reduce physical contact. There has been a momentous increase in mobile applica-

tions and online platforms that allow doorstep delivery of groceries, medicines and other products and services.

Work-from-home policy

The work-from-home policy and online meetings through Zoom, Google Meet and Microsoft Teams have been adopted across every industry and have seen a tremendous rise since the beginning of the pandemic. Many healthcare professionals and non-frontline workers, including therapists, psychiatrists and dieticians, have been conducting programmes, seminars and consultations using these platforms.

5G network in India

India is in the process of launching the 5G network. The rapid increase in the use of digital solutions demands higher speed and connectivity. The 5G network will ensure more effective and efficient teleconsultations, remote monitoring of patients and handling of patients' health data.

The 5G network will also facilitate faster transmission of large health data files and will provide better video/audio telecommunications between doctors and patients, improve the use of augmented and virtual reality and enhance the use of AI in healthcare devices.

Role of social media platforms

Social media platforms, such as Facebook, Instagram, Twitter and WhatsApp, have been very popular in India, and their use has only increased since the pandemic.

For example, when a second wave of COVID-19 hit in India in 2021 and resulted in a shortage of oxygen cylinders and hospital beds, social media platforms played a key role in providing people with information on the availability of oxygen cylinders and hospital beds around the country.

Social media platforms have also enabled patients to connect with relevant organisations such as NGOs that supply and deliver oxygen cylinders and other ICU equipment to set up at home. Additionally, many healthcare professionals and doctors in India have been consistently posting and sharing videos on social media, providing free consultations and guidance to people to tackle the virus.

Notwithstanding, the Indian government has been regularly discouraging people from taking unsolicited and unprofessional COVID-19-related advice from social media. However, many reputable health experts and physicians still continue to provide such advice on social media, which is not currently prohibited by the government. It appears that government organisations are allowing professional and genuine healthcare experts to provide COVID-19 advice on social media.

The Indian government has from time to time ordered social media platforms, including Twitter, Facebook, Instagram and YouTube, to remove posts that were fake and misleading, as well as those that were critical of its handling of the pandemic.

The Ministry of Electronics and information Technology (MEITY) enacted the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 on 25 February 2021. The Guidelines require digital media platforms to:

- implement grievance redressal mechanisms;
- appoint resident grievance officers;
- actively monitor content on the platform;

- issue monthly compliance reports; and
- adopt self-regulation mechanisms and an oversight mechanism deployed by the MEITY.

Online legal proceedings

Amid the COVID-19 pandemic, the courts and tribunals, including the Trade Marks Registry, the Patent Office and the Design Office ("IP Offices"), in India have been conducting hearings and other meetings through video conference (VC) facilities. There is even a proposal under consideration to do away with physical hearings. The adoption of VC hearings in IP offices has not only expedited the resolution of pending IP applications and opposition proceedings but has also increased the transparency of the entire process. The Delhi High Court has issued specific rules for conducting VC proceedings.

These VC proceedings have made the administrative and legal procedures much faster and efficient, allowing companies, brand owners, inventors and other stakeholders to obtain faster protection of their intellectual property and to resolve legal disputes in an effective manner.

Conclusion

Considering the country's size, demography and the size of the rural population without adequate access to the healthcare infrastructure, India has significant scope to develop advanced and affordable digital healthcare technologies and platforms. With regard to the legal regime, India has not thus far enacted a robust law on digital healthcare. Currently, India is in the process of enacting specific laws on digital healthcare, information security and personal data protection. A robust and unified digital health law may evolve very soon, given the pace of transformation in the healthcare sector.

ISRAEL

Law and Practice

Contributed by:
Eran Bareket
Gilat, Bareket & Co., Reinhold Cohn Group

Contents

Gilat, Bareket & Co., Reinhold Cohn Group is the leading intellectual property consulting firm in Israel. RCG offers the full breadth of intellectual property-related services and expertise, including protection, asset management, due diligence, and litigation and legal services. The firm operates in all areas of IP, such as patents, trade marks, designs, copyrights, open source and plant breeders' rights. The group includes the intellectual property attorneys firm Reinhold Cohn & Partners and the law firm Gilat, Bareket & Co. RCG employs over 200 professionals, out of which over 50 are patent attorneys and attorneys at law. 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. RCG and its team of professionals are internationally renowned for excellence and continually ranked amongst the top tiers in leading international and local guides.

Author

Eran Bareket is a partner at the Gilat, Bareket & Co., Reinhold Cohn Group. He holds an LLB degree, 1990, from Tel Aviv University and teaches in leading Israeli universities. Eran's expertise is litigation of IP rights, unjust enrichment, competition law and complex litigations, particularly those involving issues of technology and management of multi-jurisdiction IP litigations. Eran has vast experience appearing before all Israeli courts, including the Patents, Designs and Trademarks Registrar. He is well versed in the fields of IP, high technology, technology transfer and licensing, digital health, big data licensing, competition law, agency and distributorships, regulatory law (pharmaceuticals and medical devices), defence and homeland security, and governmental companies. Eran is often involved in the Israeli Parliament (Knesset) legislative process, acting on behalf of various entities. He serves as consultant for IP matters to the Accountant General's Division of the Ministry of Finance and represents the government regarding disputes surrounding inventions by state employees (service inventions).

Gilat, Bareket & Co., Reinhold Cohn Group

26A Habarzel St.
Tel Aviv
Israel

Tel: +972 3 567 2000
Fax: +972 3 567 2030
Email: info@gilatadv.co.il
Web: gilat-bareket.rcip.co.il/en/

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Digital health products have become an integral part of medicine, whether in the prevention, diagnosis, treatment or management of health and diseases.

From the point of view of the patients/consumers, health apps have improved their ability to track their health and fitness, store or transmit health data, keep track of their test results or doctor appointments and improve their wellness and well-being. At the same time, these technologies increase the risk of invasion of privacy and leakage of personal sensitive information.

Healthcare providers (HMOs) use digital health products to improve and enhance the quality of medical services provided. This includes, among others, decision support systems, workload management systems, telehealth services, and early detection technologies. For instance, the Director General of the Ministry of Health (MoH) recently issued a directive encouraging hospitals and HMOs to increase the use of telehealth to monitor and examine patients in order to minimise physical clinic visits in anticipation of winter 2023.

HMOs are also actively engaged in out-licensing access to their highly valuable databases of health data.

From a regulatory standpoint, the primary entities are the MoH and the Authority for the Protection of Privacy, with the Authority for Innovation and others occasionally playing a role.

Combining technological platforms with clinical evidence that measures intervention leads to considerable technological progress. A prime example is the digital surgery platform, VELYS□, which employs AI and patient-specific data collection to transform orthopedic surgery. This platform not only changes the way surgeons work, but also improves patient recovery by facilitating the creation of personalised treatment and surgery plans.

Combining technological platforms with clinical evidence that measures intervention leads to considerable technological progress. For example, the digital surgery platform VELYS□ uses AI alongside specific data collection capabilities on

each patient, and leads to a change in the field of orthopedic surgery – both in the way surgeons work and in the patients recovery through the creation of a personalized treatment and surgery plan.

1.2 Regulatory Definition

There are no regulatory definitions of digital health and digital medicine. There are several circulars of the MoH addressing certain aspects of these activities. The main body of regulation that is not health specific but that applies to digital healthcare is the privacy protection framework.

1.3 New Technologies

Some of the key technologies enabling new capabilities in digital healthcare and digital medicine are:

- sensor technologies, facilitating nano-level detection as well as various non-invasive techniques; these are particularly useful for wearables;
- AI and machine learning technologies – these are useful both for studies aimed at finding treatment and diagnostic solutions that will improve predictive medicine and personalised medicine,
- research platforms and technologies based on big data, AI, and machine learning to find treatment and diagnostic solutions and to identify new medicines and biomarkers, etc;
- decision support systems based on AI and machine learning technologies for physicians and other workers of the healthcare industry that will improve the quality of healthcare services;
- high-speed and high-bandwidth sophisticated telecommunications systems useful for both telemedicine and remote care; and
- advanced computer vision technologies that facilitate, together with AI and machine learning technologies, improved interpretation of various medical imaging devices and are currently used as decision support tools for physicians.

1.4 Emerging Legal Issues

The emerging key legal issues in digital health are explored in more detail in other sections of this chapter. Briefly put, they include privacy and data security issues, healthcare regulatory concerns such as anonymisation and preservation of confidentiality of health data, regulatory limitations on data sharing, data portability and the application of contract and commercial law to the evolving industry of data access and licensing.

1.5 Impact of COVID-19

The State of Israel has emerged from the grips of the COVID-19 pandemic, yet the pandemic's legacy continues to shape the country's healthcare landscape. The surge in digital prescriptions and other tech developments, such as telemedicine capabilities, have transformed healthcare delivery. Moreover, the pandemic has been a catalyst for the expansion of home-based medical services, enabling healthcare professionals to offer treatment beyond the confines of traditional healthcare facilities.

The impetus behind developing and adopting digital healthcare technologies was strong even before the COVID-19 pandemic. Nevertheless, the pandemic did bring about a certain acceleration because of the increased motivation, both for the public sector and the private sector, to invest financial resources into more efficient provision of healthcare services. This included telemedicine solutions, AI-based monitoring solutions (for example, a monitoring system that enables

advance prediction of respiratory complications of patients hospitalised in intensive care units or another hospital unit) and automation of digital processes. Home diagnostics devices connected to the internet enabled patients struggling to attend in-person appointments to transmit medical data on an ongoing basis to their physician.

Lastly, the highly developed infrastructure for big data studies enabled data studies of the results of the national vaccination programme that resulted in millions of people being vaccinated in a very short period of time. The results reported in prestigious magazines have enabled the global medical community to benefit from Israel's experience within a very short period of time.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

The key regulatory agency is the MoH, which is responsible for most aspects of the healthcare and pharmaceutical industries. It issues marketing authorisations for pharmaceuticals and for medical devices, including regulation of the requisite clinical trials. It also regulates the activities of the HMOs. Finally, the MoH regulates the practice of medicine by physicians. There is no separate agency that is entrusted with the regulation of digital medicine, digital health and/or medical devices.

2.2 Recent Regulatory Developments

The digital transformation of the healthcare industry is unfolding rapidly, but the development of a comprehensive and detailed digital healthcare regulatory scheme is lagging behind. The government published a national digital transformation plan and the MoH followed suit with its own digital health programme. However, primary legislation was not amended. Draft regulations (secondary legislation) relating to health data anonymisation and health data sharing have been published for public consultation but have not yet been published.

As it stands, the main regulatory documents that have been published today are circulars of the general manager of the MoH that concern certain aspects of secondary use and sharing of health data, the use of digital means in the process of obtaining informed consent, the use of cloud computing in the Israeli healthcare system, the criteria for operating telehealth medicine, providing patients accessibility to personal health data ("healthcare in the palm of your hand"), the protection of information in computerised systems in the healthcare system, the rules of ethics for remote care of Israel Medical Association, etc. The circulars are intended to be binding for HMOs and hospitals, although this is partially disputed by certain HMOs. Their authority over the private sector remains uncertain, yet due to the private sector's reliance on healthcare institution data, considerable control over conduct is largely maintained.

In early 2023, a draft bill proposing a health data portability law was introduced. The objective of this bill is to provide the necessary regulatory infrastructure to ensure patient health information is available and reviewable when and where it is needed, all the while maintaining patient privacy and information security.

To realise the vision of quality information in the Israeli healthcare system and to facilitate and improve co-operation between the authorities, a medical nomenclature project was recently launched. This project promotes the use of documentation and data coding in the Israeli

healthcare system, with the first phase involving the implementation of SNOMED-CT for uniform medical terminology to document medical operations and diagnoses.

At the data protection and privacy level, the Privacy Protection Authority has published statutory regulations covering the various aspects of data protection. The regulations were inspired by, and are generally consistent with, the European General Data Protection Regulation (GDPR).

2.3 Regulatory Enforcement

The main regulatory enforcement activity currently conducted concerns privacy protection enforced by the Privacy Protection Authority. This Authority supervises and enforce not only hospitals and HMOs, but also the Medical Examination Institute and imaging institutes, which naturally hold sensitive medical information. The pressing need for stringent oversight by the Privacy Protection Authority is clearly underscored by two key factors: the extreme sensitivity of health information and the rapid pace at which digital health solutions are being adopted, all set against a backdrop of an underdeveloped and non-systematic healthcare regulatory scheme. For example, in 2021, during the COVID-19 pandemic, enforcement actions revolved around the transfer of personal information from the MoH to the various local authorities and municipalities.

The enforcement actions of a regulatory authority can take place either on an administrative or criminal level. Administrative measures might include imposing fines or recommending the removal of officers from their posts. Before imposing an administrative sanction, the regulatory authority must gather evidence sufficient enough to justify its decision and, in most cases, must allow the institution an opportunity to present its case before a final decision is reached. On the other hand, criminal enforcement involves bringing a case before a competent court and may result in imprisonment, a fine or both.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

The Privacy Protection Authority is a non-healthcare regulatory agency responsible for enforcing the privacy and data protection legislative scheme in Israel. All other health-related issues (including wellness, fitness and self-care) are regulated by the MoH.

The Privacy Protection Authority is primarily concerned with issues, including: the way data is collected; the way data is shared; preserving the confidentiality of private data, including health data; protecting against data breaches; managing medical terminology; and preventing cyber-attacks, amongst others. The MoH is concerned with almost all aspects of the healthcare and medical industries. These include the health of patients (safety and efficacy of treatments), proper management and financial stability of health institutions, the national health budget, and the rights of patients. As such, the matter of health data usage and sharing falls under the joint jurisdiction of these two authorities. Regarding data anonymisation, the MoH typically assumes the lead role. Interactions between these two entities generally lack transparency.

Government participation is also manifested through the Authority for Innovation, which offers financial support for digital medicine projects across various fields.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

There is no significant difference between preventative care and diagnostic care under Israel's healthcare systems, since both of them are regulated under the same laws and regulations and are provided by the same healthcare providers, namely the HMOs. For example, the definition of "practice of medicine" under the Physicians Ordinance [New Version], 1976, does not differ between specific fields: "means any examination, diagnosis or treatment of, and the giving of any prescription for, sick or injured persons, attendance to women in connection with pregnancy and childbirth, and other services generally performed by a physician". Accordingly, health maintenance organisations provide a wide range of medical services, including services of preventative care, as well as of diagnostic care.

4.2 Increased Preventative Healthcare

Social trends such as people becoming more knowledgeable and active about their health during the COVID-19 pandemic, brought about an expansion of digital health. Government initiatives (such as the food labelling reform) have also contributed to health awareness and increased the focus on preventative care. Accordingly, healthcare and non-healthcare organisations began investing in the wellness field. Health maintenance organisations began to implement their services and technologies for healthcare and wellness. For example, Clalit (the largest HMO in Israel) provides its members with the "Active" app, which promotes a healthy lifestyle by recommending various personal goals, such as a daily number of steps, and other physical activity, as well as recommending how much water to drink, and providing data about sleeping patterns, and more.

Clalit also recently announced the launch of an AI platform called CPI (the Clalit protective-preventive intervention platform), which provides doctors with data regarding which patients would benefit from preventive medicine due to certain risk factors.

Israel is a leading country in preventative care. One of the fields in which Israel invests is food technology. For example, in 2020 the Inaugural Global Wellness Summit Prize for Innovation was awarded to Amai Proteins, an Israel-based innovator that developed protein-based products for food and beverages, including a sweet designer protein as a substitute for sugar ("designer sweet proteins"), that significantly reduces added sugar in a wide variety of food and beverages. The awareness of preventative care is constantly rising, leading to the development of new technologies that promote a healthy lifestyle.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Wellness and fitness data are not subject to specific healthcare or privacy regulations, but rather to general regulations that apply to data and digital health (see a list of relevant regulations in **4.1 Preventative Versus Diagnostic Healthcare**).

In addition, 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; and
- GD Circular dated 11 November 2019, regarding patient access to personal health data – "Healthcare under your Control."

- GD Circular dated 15 December 2019, regarding the management of patient records in the health system;
- GD Circular dated 5 January 2020, regarding the code of ethics for maintaining the confidentiality and integrity of personal information;
- GD Circular dated 21 February 2021, regarding the use of cloud computing in the health system;
- GD Circular dated 30 November 2021, regarding recommendations to the public in the use of wearable devices for sports and health purposes; and
- GD Circular dated 13 March 2022, regarding cyber protection in the health system.

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 for secondary use will be anonymised. Furthermore, any secondary use of health data for research purposes must be pre-approved by the Helsinki Committee.

No law in this field has been developed by courts or judges, but rather by legislative enactment.

4.4 Regulatory Developments

To date, no binding regulation applying specifically to preventative healthcare has been enacted in Israel.

4.5 Challenges Created by the Role of Non-healthcare Companies

The digital healthcare market's landscape is in constant flux, and there are many areas of uncertainty; it may also vary among countries. Thus, partnering with an institution with experience in the field is advantageous. Special attention must be paid to the regulatory schemes applicable to both the R&D stage, as well as to the commercial marketing and sales stage.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

The following have enabled the enhanced use of connected devices in digital healthcare:

- technologies of telehealth;
- wearable electronics that allow user data capture;
- AI/machine learning that enable user data processing, analysis, diagnostics and prediction;
- a cloud that allows remote monitoring of patients; and
- robotics that allow performance of certain tasks in hospitals and assisted surgery.

At the end of 2021, the Authority for the Protection of Privacy published a document of recommendations concerning the use of wearables for sports and health purposes.

In this regard, Clalit provides its members with the "TytoHome" device that can be used at home, through which doctors can remotely perform a live examination and provide a diagnosis, treatment notes, and any referrals or prescriptions. The TytoHome kit allows for detailed health readings on critical areas of the body, such as the heart, lungs, ears, throat, abdomens and skin, as well as heart rate and body temperature. Another example is the CardioSen'C device of SHL, a portable device that monitors heart activity, and which can communicate the results instantaneously to a cardiologist.

5.2 Legal Implications

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.

5.3 Cybersecurity and Data Protection

When using a cloud computing environment, questions arise regarding the privacy and security of the data uploaded to the cloud. 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 the theft of patient medical data and the risk of cyber-attacks. Oracle 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.

The health sector was one of the ten most cyber-attacked sectors in Israel in 2021. Accordingly, in 2022, the MoH published basic principles for the regulation of cyber defences in the healthcare system alongside principles for integrating remote medicine systems into emergency medical centres. Furthermore, the Ministry of Justice and the Authority for the Protection of Privacy published a document concerning the protection of patient privacy in telemedicine services. On May 2023, an annual report of the state auditor on cyber and information systems was published, following a cyber-attack on Hillel Yaffe hospital in Hadera that occurred in mid-October 2021.

As to the local computing environment, concerns regarding the privacy and security of uploaded data still exists but can be minimised by setting forth and implementing data security standards. The Protection of Privacy Regulations (Data Security) 5777-2017 states that, in the event of a contract between a database owner and 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.

The health data circulars 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 anonymised. Furthermore, the circulars set detailed conditions for privacy, medical confidentiality, standards for managing patient records in the health system, and data security.

5.4 Proposed Regulatory Developments

To date, there are no specific proposed regulations or regulatory guidance in the field of the internet of medical things.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Unfortunately, there is no statutory definition of software as a medical device. The registration of medical devices is entrusted to the medical accessories and devices (MAD) unit of the MoH. It must be noted that there is no legal requirement to obtain marketing approval for medical devices. The MAD unit nonetheless operates because HMOs and hospitals will not purchase non-approved devices. The MAD unit recognised US (510K) and EU (CE) approvals, meaning that holders of such approvals can easily obtain authorisations in Israel as well.

In December 2022, the MOH published a request to receive input regarding guiding principles for the development of AI-based technology in the digital health sector. The request was based on a similar request from the FDA in 2019 (Good Machine Learning Practice for Medical Device Development: Guiding Principles). The input received is currently being reviewed.

7. Telehealth

7.1 Role of Telehealth in Healthcare

To date, telehealth has been more widely used in Israel in some fields. However, just recently, in August 2022, the Authority for the Protection of Privacy published a document of key recommendations on the provision of remote medical services.

Patient-physician consultations through video calls have become popular but primarily after hours (through central service centres). Remote monitoring by means of handheld medical devices carried by patients in their homes has also become popular. This device not only monitors certain indices but also allows the physician to (partially) inspect the patient as if the patient were in the clinic, and to receive medical data obtained by remotely monitoring the patient using sensors. Surgeries have been conducted in hospitals with the participation of foreign experts through video calls. Virtual hospitals have not yet been established.

One of the concerns raised in the context of telemedicine is the digital divide and the concern that certain populations will be discriminated against and not be able to benefit from these new services.

As yet, there are no special regulations for cross-border provision of services and the general rules apply (meaning that non-licensed practitioners cannot provide health services from abroad).

7.2 Regulatory Environment

During the COVID-19 pandemic, certain relaxations of the regulatory scheme were made. For example, the guidelines regarding clinical trials were modified and relaxed in several aspects with a view to achieving social distancing during the informed consent process, and during meetings to discuss and approve the conduct of clinical trials, etc. Notably, studies on health data were exempted from certain approvals if the data was anonymised. All such relaxations were cancelled after the pandemic subsided.

7.3 Payment and Reimbursement

Almost all healthcare services are provided by the four major HMOs. The HMOs are funded by the government based on the number of patients they treat. The HMOs are generally not required to provide drugs and medical services not funded by the government. Each year, a special committee approves the introduction of new drugs and new technologies to the "healthcare basket", thereby requiring the HMOs to provide such solutions.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

A host of technological developments have enabled the internet of medical things (IoMT) to develop to its current stage. One could begin with continuous improvements in authentic communications infrastructure (culminating in the recently introduced 5G network technology) that facilitates connectivity and bridges geographical gaps, improvements in computer vision, as well as various imaging techniques, coupled with the miniaturisation of chips and other hardware components, the increased computational power of computers, the development of highly sophisticated sensors (in particular, non-invasive wearable ones), the improvement in energy storage and battery life, and the maturity of machine learning and AI as applied to health data, to name just a few of the driving technologies.

The development of IoMT facilitates a wide scope of functionalities, such as remote monitoring; remote measurements of patients' indices, such as pacemaker monitoring, infusion pumps, insulin pumps and implant condition monitoring; as well as control and management of available resources and assets, building control and monitoring the environment of patients.

However, the growing use of these components and technologies results in increased exposure to cyberthreats, privacy risks through the exploitation of existing vulnerabilities, hostile takeovers and the like.

In order to assist health organisations in addressing these risks, the National Cyber Authority published in late 2020 a guide entitled "IoMT-Based Medical Device Protection Recommendations", which concerns actions and controls to strengthen IoMT devices, while making recommendations for dedicated controls. The guide builds on classifications published by the Cloud Security Alliance (Managing the Risk for Medical Devices Connected to the Cloud). As it states, it should be remembered that there is no single technology applicable for all types of systems. Therefore, cyber protection for IoMT components has necessitated requirements for the protection of such components as well as protection from them. Also, a variety of components are provided by a variety of vendors and not everyone comes with the same security settings. These facts make it difficult to create standardisation and uniform component management. This results in a need to protect IoMT components and their environments while combining different controls (policies, technologies, code, and hardware).

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

The introduction of 5G networks is expected to have a major beneficial impact on the healthcare industry. Owing to its high bandwidth, high

speed and improved latency and error rate, 5G technology is expected to:

- be more secure and reliable;
- better facilitate remote monitoring and telemedicine;
- enable sophisticated surgeries conducted from remote locations and improved machine learning capabilities, particularly with respect to large image files;
- enable high computing power to mobile devices dependent on communications;
- obviate the need for close proximity between machine learning servers and data sets; and
- facilitate global immediately available medical consultation and other similar improvements.

The deployment of 5G networks in Israel is slowly progressing. As part of the activity and enforcement plan of the Authority for the Protection of Privacy in preparation for the deployment of the network, adjustments are also required regarding digital health and TELEHEALTH applications.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

The key legal issues in using and sharing personal health in research and clinical settings are as follows.

- Compliance with the requirements imposed by the privacy protection regulatory scheme. These include the maintenance of appropriate data security protocols, the use of collected data solely for the purpose declared upon collection, and the registration of databases containing sensitive health information.
- On 7 May 2023, new regulations were adopted with stricter instructions that set a higher bar for maintaining information that came from the EU.
- Compliance with the requirements imposed by the MoH regarding the use and sharing of health information. These include the requirement to maintain the anonymity of patients through anonymisation, aggregation and sometimes the use of synthetic data; the need to obtain approval for the conduct of clinical trials as big data research is considered a type of clinical trial requiring pre-approval; limitations on the grant of exclusivity for conducting big data studies; certain limitations on the permissible nature of big data studies; and requirements pertaining to their contractual undertakings for entities wishing to have access to health data in order to conduct studies, etc.

There are no different regulatory frameworks for data use or for data sharing. The distinction made is between primary use, which is use of a person's health data (including identifiable data) substantially for the purpose of treatment of that particular individual, and secondary use, which is defined as any other use. Primary use does not require the patient's consent. Secondary use requires either the patient's informed consent (opt-in) or the use of anonymised data (which, if done properly, means a patient's consent does not need to be obtained).

In this context, the MoH recently launched the "World of Data" platform, which allows the public to see a broad picture of the health system and the quality of its medical care.

Alongside this, a national platform was launched for conducting big data research in health data (research infrastructure for huge data). The plat-

form is intended to serve the research community in conducting groundbreaking research in the field of health, by collecting health data from HMOs, but it faces difficulties and considerable barriers with regards to its implementation.

There are cases when the comparison of anonymised data with other data sources can result in re-identification. When access to the other data source requires informed consent (such as genetic data), the patient will typically be requested to provide consent to access their other phenotypic data. Alternatively, the database holder (eg, the HMO) will provide the researcher with unique keys that enable only the HMO but not the external researcher to connect and then analyse data with the identified data of the patient.

Informed consent may be obtained either by traditional means or by digital means. When digital means are used, this must be done in a procedure published by the MoH in October 2020. The general rule is that there must be a face-to-face meeting between the participant in the trial and the researchers. However, such a meeting can be conducted virtually and not necessarily in person. When choosing whether to make use of digital means in the process of obtaining informed consent, one must examine, among other things, the balance between the benefit of using such means and the associated risks, the severity of the medical intervention in the clinical trial, the characteristics of the target population and their level of access to the proposed digital means, the number of participants and their level of access to the place where the trial is conducted.

One declared goal of the procedure is to prevent the exclusion of various populations, particularly in light of the digital divide. Lastly, when asking a patient to opt in to participate in studies and activities that do not have direct benefits for such person, it is preferable to obtain their opt-in consent through a special recruiter instead of the attending physician.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

The regulatory scheme mainly addresses the issues of data security, data sharing, secondary use, accessibility to personal health data, ethics and anonymisation. It does not yet regulate the utilisation of AI and machine learning in general or the digital healthcare industry in particular.

Machine learning is particularly useful in the healthcare industry in research fields such as computer vision (the analysis of images for the purpose of diagnostics); associations between phenomena that are useful, for example, for drug repurposing and identifying novel indicators useful to predict illness; and harnessing collective wisdom, namely by creating algorithms for decision support systems that match or even outperform the output of large peer consultations.

One of the challenges for training machine learning algorithms is the need for access to sufficiently large and representative data sets and the need for removing bias underlying past decisions studied by the algorithm. Luckily, the data sets of the two large HMOs in Israel are relatively large. Nevertheless, when a particular research topic requires the pulling of data from different sources, the process is still cumbersome. Another limiting factor is the need to have geographical proximity between the machine learning server and data set.

Natural language processing (NLP) is particularly useful in big data analysis of interactions between a physician or a therapist and their patient. NLP may also be useful in the digitisation of handwritten records.

Research involving genetic data poses substantial privacy risks due to its inherent sensitivity. While in other use cases, such as studying medical conditions, the risk lies in the potential for an attacker to connect the data to a specific individual, genetic data takes this a step further. The genetic data inherently pertains to the individual's identity, making it a high-risk category for sensitive information misuse.

11.2 AI and Machine Learning Data Under Privacy Regulations

To date, there are no specific enacted regulations that address the use of AI and machine learning data in healthcare.

However, an Artificial Intelligence and Data Science Committee was appointed in February 2020 by TLM (the Forum for National Infrastructures for Research and Development), with the aim of examining the need for government intervention to accelerate the development of Artificial Intelligence and Data Science.

The committee recommended that future regulation in the field of AI should address the following:

- "Enabling regulation", namely a regulation that enables a rapid technological development that is not slowed down by out-of-date regulation;
- standardisation and legislation of algorithms, models and data;
- purchase and sale policy of algorithms and products, especially regarding products of the security forces;
- establishment of data centres and platforms for data sharing and models; and
- data management, cybersecurity and information protection.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Companies that develop and sell new digital healthcare technologies must comply with the provisions of the health data circulars, as well as with the provisions of the law and the privacy regulations (if the technology collects personal data).

Agreements with public healthcare companies require that special attention be given to the regulatory environment of the healthcare entity (eg, an HMO):

- Public-regulated healthcare entities are limited in their ability to hold equity in non-healthcare companies.
- Public-regulated healthcare entities are restricted in their ability to accede to requests for non-compete/exclusivity arrangements.
- Healthcare organisations involved in the development of new technologies will typically consider implications of 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.

In general, the lack of stringent digital health enforcement in Israel creates a more accessible landscape for the digital healthcare market.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

The IT infrastructure of the HMOs providing care to the majority of the patient population in Israel is well developed to support digital healthcare. The same is true for the main large hospitals. Some of the challenges ahead include:

- commonly accepted standardisation of classification of clinical data;
- digitisation of old records;
- data curation;
- establishing infrastructure and promoting participation in platforms for the pulling of clinical information; and
- securing the resources necessary to recruit patients when opt-in is required, such as genetic and bio-sample studies.

13.2 Data Management and Regulatory Impact

To date, there are no specific proposed regulations or enacted regulations regarding the implementation of IT upgrades. In general, the manner in which data is managed 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) and the health data circulars aimed at regulating secondary use of health data and big data research.

14. Intellectual Property

14.1 Scope of Protection

Patents are generally available for any invention that is a product or a process in any technological field that is novel, non-obvious, useful and capable of industrial application. A noteworthy exception to patentability is the prohibition of patents for a process of medical treatment of humans. This exception, coupled with case law trends concerning patentable subject matter, sometimes creates hurdles in pursuit of patent protection for inventions relating to personalised medicine. The territorial limitation of patents (patents being enforceable only within the territory of the country where they were registered) requires careful drafting of claims of patents relating to ex vivo diagnostics of medical conditions.

Copyright protects software as a literary work, but such protection generally extends only to the way of expression rather than the functionality and technological ideas underlying the code. The latter should be protected by patents where possible. Data sets are generally not protected by copyright and there is no sui generis database protection in Israel.

Trade secret protection is available in Israel and may protect confidential information, including non-patentable inventions and non-copyrightable data sets. However, in order to benefit from such protection, the information must be kept confidential, and the owner of the confidential information must show that they took reasonable efforts to protect the confidentiality of the trade secrets. Reverse engineering, as such, is permissible.

There is no case law, as yet, regarding inventions and works of authorship created by AI technologies without direct human contributions. How-

ever, it would seems that any person who was involved in the process of creation and has provided inventive contribution to the inventive concept of the invention (under the classic inventorship criteria) should be deemed an inventor.

14.2 Advantages and Disadvantages of Protections

In general, IP rights in the field of healthcare are difficult to enforce, since there is a convention that healthcare should be for the benefit of the public and enforcing rights in this field can be deemed as harming access to health.

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, are not patentable per se, 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.

There are some difficulties in protecting software and algorithms, since, on the one hand, patentability issues may arise, and, on the other hand it is difficult to enforce such rights from the evidentiary aspect (to prove that the competitor copied the code).

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 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.

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:

(i) taking a trade secret without the owner's consent by improper means, or the use of the secret by the acquirer;

(ii) 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

(iii) 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 (i) or (ii).

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 but the requirement of keeping it "not easily disclosed by others" can be difficult while using AI technologies.

14.3 Licensing Structures

The health data circulars set forth the provisions to be included in collaboration agreements based on secondary uses of health data (such as the purpose of using the data or maintaining the confidentiality of the data). In general, 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.

In general, HMOs request monetary considerations and rights to use the products, based on use of the data they grant access to. The issue of royalty-stacking may arise, leading to a burden of royalties to be paid by start-ups.

14.4 Research in Academic Institutions

Employers, including universities and healthcare institutions, will generally be the owners of IP rights generated by their employees in connection with their employment. This is both in terms of the default rule under the Patents Law and the Copyright Law, as well as the standard practices of such organisations, which often expand beyond the statutory provisions by means of employment contracts and intellectual property by-laws. All academic institutions share the revenues collected by the commercialisation of such intellectual property with the researchers. HMOs differ in their approaches and practices. The allocation of IP rights when private sector technology companies are involved in developing the device or medical innovation is typically governed by contract. Special provisions apply to governmental hospitals, which are more limited in their ability to contract with the private sector.

14.5 Contracts and Collaborative Developments

The default rule is that any person who made an inventive contribution to the inventive concept of the invention is an inventor and is the owner of the invention. When there are several co-inventors, they will be co-owners (unless they are in the employ of a third party, in which case the employer will own a share of the invention). All of these default rules may be superseded by contract.

It is standard practice to distinguish between background IP and foreground IP, with ownership of the background IP remaining with the original owner, who may grant limited licences to use the background IP in order to exploit the foreground IP, and the foreground IP being owned as agreed by the parties. Because of regulatory constraints and other considerations, many HMOs will waive co-ownership in exchange for various monetary rights, such as royalties, milestone payments, exit phase, cross-licence or the right to use the resulting foreground IP.

15. Liability

15.1 Patient Care

The first theory of liability arising from decisions based on digital health technologies such as data analytics, AI, machine learning and software as a medical device is, of course, the tort of negligence. In general, the three main elements of this tort are the existence of a duty of care, deviation from a reasonable standard of practice, and a causal connection between the defendant's act or omission and the damage suffered by the plaintiff. The manufacturer of a medical device will generally be held to owe a duty of care towards users of the device. Adherence to acceptable standards should mitigate the risk of liability. Otherwise, the manufacturer will have to show that it took reasonable efforts to prevent the damage, with the foreseeability of the damage and the level of efforts required being directly related, namely, the more foreseeable the damage is, the higher the level of efforts required.

It is hard to see how a decision to use an approved medical device can be deemed negligent. However, a decision to use a medical device in development could theoretically attract liability and the putative defendant would have to show that they took reasonable measures to verify that the device's algorithm would not cause harm or produce misleading results. As is the case with other industries, the courts will have to acquaint themselves with the developing best practices that aim to deal with the problem of lack of transparency of machine learning algorithms.

If a medical device inflicted physical damage on a patient, the manufacturer of the device may be held liable under the Defective Product Liability Law, which imposes a strict liability (no fault) on the manufacturer.

15.2 Commercial

Theories of liability when third-party vendors' products or services cause harm to healthcare institutions are generally the same as those discussed in **15.1 Patient Care**. The main difference, however, is the ability of the healthcare institution to protect itself through contract by obtaining proper warranties and indemnification obligations. In addition, health institutions may forfeit at least part of the right for compensation if they are shown to have breached their obligation to mitigate damage. Thus, some institutions already proactively monitor their internet-connected equipment to detect vulnerabilities and prevent cyber-attacks.

JAPAN

Law and Practice

Contributed by:
Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi
Anderson Mori & Tomotsune

Contents

JAPAN CONTENTS

Anderson Mori & Tomotsune is a large, international Japanese law firm. The firm is known for its long history of advising overseas companies doing business in Japan and in cross-border transactions. The main office in Tokyo is supported by offices across Japan, China and the South-East Asian region. Anderson Mori & Tomotsune has considerable experience in matters relating to the life sciences field, including expertise in licensing, regulatory, intellectual property and corporate transactions such as M&A and venture investments. The firm works with increasingly diversified international and Japanese-based healthcare companies, including pharmaceutical manufacturers, medical device manufacturers, distributors and e-health providers. The team, which consists of about ten partners and 20 associates, provides comprehensive advice from the set-up of a Japanese entity to all stages of the product life cycle and helps clients to navigate a broad range of regulatory matters.

Authors

Junichi Kondo is a partner at Anderson Mori & Tomotsune. His practice focuses on corporate, M&A and regulatory affairs involving the pharmaceutical and medical devices industries. He regularly advises both local and foreign clients on M&A of listed and unlisted businesses and joint ventures. He also regularly provides advice on general corporate and commercial matters and regulatory affairs, including licensing, dealings with healthcare professionals, labelling and promotion, off-label use and adverse event reporting. He is a member of the Dai-ni Tokyo Bar Association (Japan) and admitted to the New York Bar. He is widely published in the field of life sciences.

Yasufumi Shiroyama is a partner at Anderson Mori & Tomotsune. He has focused on global and domestic dispute resolution of intellectual properties in various forms, including patent and trade secrets, as well as having advised on transaction and regulatory matters in relation to life sciences and other technologies. In addition, he has taught at the University of Tokyo, School of Law since 2004 and was a chairperson of the JFBA Committee on Intellectual Property Rights in 2017–18.

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

Hiroshi Ishihara is a co-head of the healthcare, pharmaceutical and life sciences department at Anderson Mori & Tomotsune. In his practice in the life sciences area, he handles commercial transactions, such as M&A of pharmaceutical companies and licence agreements. He also advises clients on regulations related to drugs, medical devices and regenerative medicine. He is an adviser of the Medical Affairs Study Group of the Japan Pharmaceutical Industry Legal Affairs Association. Hiroshi is a qualified Japanese lawyer (bengoshi) as well as a qualified lawyer in New York and California.

Masayuki Yamanouchi is a partner at Anderson Mori & Tomotsune. He holds a Master's degree in science and has been engaged in various matters involving technology issues. His main focus is on the pharmaceutical industry, and he has advised both domestic and foreign clients on pharmaceutical regulations and has represented clients in patent-infringement actions, as well as licensing negotiations, joint-development projects and technology-transfer projects. He also has expertise in AI and big data-related technologies applied in medical services and products. Masayuki is a member of the Dai-ni Tokyo Bar Association (Japan) and admitted to the New York Bar.

Anderson Mori & Tomotsune

Otemachi Park Building
1-1-1 Otemachi
Chiyoda-ku
Tokyo 100-8136
Japan

Tel: +81 3 6775 1000
Email: inquiry@amt-law.com
Web: www.amt-law.com/en

ANDERSON MŌRI & TOMOTSUNE

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Definitions of Digital Healthcare and Digital Medicine

While Japanese law does not provide formal definitions of digital healthcare and digital medicine, there is a difference in those terms based on whether a product constitutes a "pharmaceutical" or a "medical device" under the Securing Quality, Efficacy and Safety of Products including Pharmaceuticals and Medical Devices Act (the "Pharmaceuticals Act"). Digital medicine may be viewed as relating to products that have been approved by the relevant authorities in Japan, such as the Ministry of Health, Labour and Welfare (MHLW), as a pharmaceutical or medical device, while digital healthcare may be viewed more broadly as relating to those products and services that do not constitute pharmaceuticals or medical devices and, therefore, do not require approval from the MHLW.

Difference From the Regulatory Perspective

The aforementioned differences are important because if a certain product constitutes a pharmaceutical or medical device under the Pharmaceuticals Act, the provider of that product must obtain the relevant licence, such as a marketing licence, a manufacturing licence and/or a distribution licence, and must also obtain marketing authorisation, certification or notification for the product in question.

Difference From the Patient's/Consumer's Perspective

From a patient's perspective, if a doctor prescribes a pharmaceutical item at a medical institution, the patient's cost for that pharmaceutical will be covered by national health insurance, and the patient will be required to pay only a portion of the cost of that pharmaceutical. By contrast, if a digital healthcare product does not constitute a pharmaceutical item, the consumer must pay the full price of the product to the provider.

Determination of a Medical Device

Sometimes, it can be difficult to determine whether a certain product, such as a medical-device program, may be categorised as a medical device; as such, the MHLW issued the Guideline Concerning the Determination of Software as a Medical Device on 31 March 2021 (amended on 31 March 2023; the "SaMD Guideline").

The SaMD Guideline clarified that a program that records, stores and displays personal health data for the purpose of a user (ie, a patient) monitoring their own health information does not constitute a medical-device program. By contrast, a program that is intended to diagnose, treat or prevent a disease is a medical-device program.

1.2 Regulatory Definition

Definitions and Regulations Under the Pharmaceuticals Act

As previously stated, Japanese law, including the Pharmaceuticals Act, does not provide formal definitions of digital healthcare and digital medicine.

However, the Pharmaceuticals Act contains definitions of "pharmaceutical" and "medical device," which include medical-device programs.

In general, a product or instrument (including a computer program) that is intended for use in the diagnosis, treatment or prevention of disease in humans would constitute a "pharmaceutical" or "medical device" under Article 2, Items 1 and 4 of the Pharmaceuticals Act.

Thus, if a digital medicine product is classified as a pharmaceutical or medical device under the Pharmaceuticals Act, that product would be subject to the relevant regulations under that Act. However, if a digital medicine product or a digital healthcare product is not classified as a pharmaceutical or medical device under the Pharmaceuticals Act, that product would not be subject to that Act and only the general regulations relating to a general consumer product would apply.

1.3 New Technologies

Use of Internet and Artificial Intelligence

Technologies using the internet and artificial intelligence (AI) have been adopted in digital healthcare products and medical device programs.

There are many digital healthcare products, such as applications for smartphones, that use the internet to transmit healthcare information among users.

Also, some medical device programs adopt AI for their functions to enhance their effects, such as diagnosis of a certain disease.

1.4 Emerging Legal Issues

From Face-to-Face to Online

Due to new technologies, medical treatment and medication counselling may be conducted remotely by using information communications equipment. However, medical treatment and medication counselling have traditionally been conducted on a face-to-face basis, so the existing regulations had to be amended to regulate remote medical treatment and remote medication counselling appropriately. In this regard, the MHLW issued Guidelines for Appropriate Performance of Online Medical Treatment, dated March 2018 (amended in March 2023). Also, the Pharmaceuticals Act was amended as of September 2020 to allow online medication counselling under certain conditions.

1.5 Impact of COVID-19

Online Medical Treatment and Medication Counselling

Due to the spread of COVID-19, the MHLW temporarily relaxed regulations regarding online medical treatment and online medication counselling on 10 April 2020.

Accordingly, under certain circumstances, a doctor may conduct a patient's first medical examination remotely and provide online medical treatment to that patient using information communications equipment.

Also, under certain circumstances, a pharmacist may conduct online medication counselling by telephone or through information communications equipment.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

Business Licences and Marketing Authorisation

As a general rule under the Pharmaceuticals Act, any person intending to market a medicinal product must have a business licence and obtain a marketing authorisation, certification or notification, depending on the risk classification for the product.

The MHLW has primary jurisdiction over matters concerning pharmaceuticals, medical devices, medical treatment, health insurance and other healthcare matters, including matters in the digital health sector. Authority over matters concern-

ing clinical trials, authorisations, registrations and post-marketing safety measures of pharmaceuticals and medical devices is delegated from the MHLW to the Pharmaceuticals and Medical Devices Agency (PMDA), an organisation established under the Law for the Pharmaceuticals and Medical Devices Agency. Furthermore, the granting of business licences that are required for the manufacture, marketing or sales of pharmaceuticals and medical devices, and the monitoring activities in relation to those licences, including violation of advertising regulations, is partially delegated to local governments.

In brief, the procedure for obtaining marketing authorisations for medicinal products is as follows.

Clinical trials must be performed to collect data that is necessary for the application. In essence, clinical trials performed prior to the application include:

- Phase I (for a small number of healthy adults);
- Phase II (for a small number of patients); and
- Phase III (for a large number of patients).

After clinical trials, any person intending to market a medicinal product must file an application with the PMDA for approval to market that product. The PMDA reviews and examines the application and reports the results of its review to the Minister. The Minister then decides whether to grant the approval to market the product, based on the report of the PMDA.

Reimbursements Under the National Health Insurance System

The National Health Insurance System (NHIS) is a public healthcare system that covers the entire country. Under the NHIS, everyone in the country is, in principle, entitled to all types of medical care services (including medical treatments and drugs) provided by medical institutions. Patients receive treatment at a medical institution and pay a portion (10% to 30%) of the cost of treatment at that medical institution. The remaining cost is billed to the assessment and payment agency, which reimburses the medical institution from the insurance premiums collected from the insured by the health insurance association, with the government covering any deficit.

The MHLW Welfare Ordinance prescribes the coverage by the NHIS for medical examinations, diagnoses or treatment and usage of pharmaceuticals and medical devices, including digital health products or services. Insurance reimbursement for medical devices varies, depending on the category of the device. For example, the cost of certain products, primarily disposable products, is specifically reimbursed as for pharmaceuticals. More commonly, however, the cost of the medical device is included in the medical diagnosis or treatment fee. For example, the use of software that processes image data of the human body taken by an imaging device is assessed as a technical fee in connection with a medical diagnosis. In other words, insurance reimbursement is provided for the act of diagnosis using specific software, not for the purchase or payment of a service fee for the software. Insurance reimbursement is also available for online medical treatment.

2.2 Recent Regulatory Developments

Software as a Medical Device (SaMD)

Whether certain software is regulated as a medical device under the Pharmaceuticals Act is often a nuanced question. The SaMD Guideline is the latest guideline on whether certain software should be regulated as a medical device under the Pharmaceuticals Act, and indicates how to determine whether a software is deemed

a medical device. See **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies** for details.

Telemedicine

The provision of medical diagnoses over the telephone, by video or using other online tools (online medical treatment) is becoming more common in Japan. However, the Medical Practitioners' Act prohibits doctors from providing a diagnosis without examining a patient. Thus, the issues of whether an online examination may be construed as the examination required under the Medical Practitioners' Act, and of the extent to which an online examination is permitted, are controversial. The MHLW has been accepting online medical treatment, but with certain requirements, such as that the initial medical examination be held face to face.

In 2020, however, the MHLW issued Temporary and Exceptional Measures for Medical Treatment Using Telephones and Other Communication Tools Under the Spread of the COVID-19 Infection, which temporarily permitted the online performance of a patient's initial medical examination. Now, a patient may receive medical treatment online even if they have never been examined at a hospital for the specific disease or symptom. See **7.2 Regulatory Environment** for details.

2.3 Regulatory Enforcement

The MHLW, and prefectural governments as delegated by the MHLW, have vast authority in enforcing the regulations. That authority includes the ability to issue various administrative orders against regulatory violations, such as:

- a revocation of a marketing authorisation and/or business licence;
- a business suspension order;
- a temporary suspension of sales and disposal of stocks; or
- a recall order.

Certain violations of the Pharmaceuticals Act – such as violation of administrative orders, the sale of unauthorised drugs or medical devices and off-label promotion – are also subject to criminal penalties.

Regulators use these administrative orders and criminal penalties, but sometimes only administrative guidance, based on the severity of the violation and the risk to national health. There is no other significant trend or tendency in regulatory enforcement.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

Whether a certain digital health product or service is regulated by the Pharmaceuticals Act, the Medical Practitioners' Act or the Medical Care Act makes a substantial difference. Once the relevant product or service is determined as falling outside the healthcare regime, the applicable regulations are significantly less stringent than the laws described above, though there are still some notable regulations.

The Act Against Unjustifiable Premiums and Misleading Representations, administered by the Consumers Affairs Agency, governs all consumer products, including digital health products and services marketed towards consumers. The Act prohibits any representation in which the quality of a product or service is portrayed as being significantly superior to the quality of the

actual product or service, and any representation regarding price or any other term of a product or service that could be misunderstood to be significantly more advantageous than the term of the actual product or service. Medical devices and other products governed by the Pharmaceuticals Act are also governed by this Act, but in most cases the promotion and advertising rules under the Pharmaceuticals Act are stricter than the corresponding rules under the Act Against Unjustifiable Premiums and Misleading Representations.

Further, a health-related product or service that would, by its nature, not be regulated as a medical device or a medical service may be regulated as such if an advertisement, sales promotion or other communication portrays the product or service as applicable for use in diagnosis, treatment or prevention of diseases. In this respect, the Pharmaceuticals Act, the Medical Practitioners' Act and the Medical Care Act limit advertisements and other communications regarding non-medical devices and services.

The Electric Appliances Safety Act may apply to some categories of electrical appliances. Manufacturing or importing those electric appliances requires notification to the Ministry of Economy, Trade and Industry, and the products must conform to designated technical standards.

Privacy is one of the most crucial issues relating to digital health-related services. The Consumer Affairs Agency also plays an administrative role in the privacy regime. See **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information** for details.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

The Pharmaceuticals Act defines a medical device as an instrument that is intended for use in the "diagnosis", "treatment" or "prevention" of disease. Similarly, an item that is intended for use in the "diagnosis", "treatment" or "prevention" of disease can be categorised as a pharmaceutical under the Act. Therefore, when developing an instrument or an item that can be used to prevent disease, it should be carefully determined whether the instrument or item falls within the category of a medical device or a pharmaceutical, which are subject to the Pharmaceuticals Act.

Also, only a medical practitioner may engage in medical practices under the Medical Practitioners' Act. Thus, if a certain act involves a medical intervention, such as surgery, it cannot be performed via a computer or by a layperson – only by a medical practitioner.

4.2 Increased Preventative Healthcare

Due to the increasing cost of medical care in Japan, the Japanese government, as well as private enterprises, are focusing more on measures to help people live healthy lives and prevent early onset of serious diseases. While developing pharmaceuticals requires enormous amounts of money and time, developing an instrument or software that can promote better health requires fewer resources. Therefore, many start-up companies and traditional companies, whose core business is not healthcare, are now entering the healthcare sector by developing instruments or software that can be used for preventative medicine.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Under the Act on the Protection of Personal Information (APPI), medical information is classified as "special care-required personal information", and care must be taken when handling such information. In order to acquire special care-required personal information, it is necessary to obtain the prior consent of the individual concerned, except for certain exceptions. Fitness and wellness information not classified as special care-required personal information can be acquired without the prior consent of the individual concerned. If the information is a combination of medical information and fitness and wellness information, the entire information would be classified as special care-required personal information. There have been no court precedents that have explicitly ruled on the handling of such combined information.

4.4 Regulatory Developments

As it is often difficult to differentiate between a software program that should be categorised as a medical device and one that is not a medical device, the authorities are developing a guideline and a list of examples to help a company that develops such a program determine whether its software program should be categorised as a medical device or not.

For example, a program to be used personally at home to record an individual's healthcare status for fitness purposes is not categorised as a medical device, so it is not subject to the Pharmaceuticals Act.

4.5 Challenges Created by the Role of Non-healthcare Companies

As pharmaceutical and medical devices are highly regulated by the Pharmaceuticals Act and other relevant regulations, it is often a challenge for a company that is new to the healthcare business. Such companies tend to join forces with a traditional healthcare company that has already obtained the necessary licences and approvals. Alternatively, a new entrant first develops a device or product that is not categorised as a medical device or a pharmaceutical so that they do not have to obtain and maintain the requisite licences or approvals, which tend to incur substantial costs and time.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

The internet of medical things (IoMT) and connected devices have completely changed the medical scene. They are extremely useful for in-hospital use. Radio frequency identification attached to specimens such as blood or urine samples are now indispensable for preventing mix-ups. A recently developed bed can monitor the patient's vital signs and transmit the data to the hospital's central computer system. These devices are, however, most notable for in-home use. Wearable devices enable continuous and real-time monitoring of outpatients. One Japanese pharmaceutical company has developed a drug with a microsensor to enable monitoring of the patient's compliance with dosing instructions.

5.2 Legal Implications

There is no specific legislation or other rules governing liability in the case of health injury arising from IoMT or connected devices malfunctions. There has been no case law establishing any specific rule for such liability, either.

The Product Liability Act (PLA) governs product liability litigation, along with the Civil Code. The liability under the PLA can be regarded as "strict" liability as, by replacing "negligence" with the existence of a "defect," victims are not required to prove the negligence of the manufacturer. Nevertheless, victims still have to prove the defect and the other conditions for tortious liability (namely, the existence of damage and the causation between defects in the product and the damage) to claim the damage under the PLA.

A defect is defined as a lack of safety that the product should ordinarily provide, taking the following into account:

- the nature of the product;
- the ordinarily foreseeable manner of use of the product;
- the time when the manufacturer delivered the product; and
- other circumstances concerning the product.

The claimant bears the burden of this proof under the PLA. However, a court may lower the burden of proof regarding the existence of a defect, depending on the parties involved (eg, in the instance of a consumer acting against a large corporation), the nature of the product (such as the complex operational functions of a product) and the ordinarily foreseeable manner of use of a product.

Under the PLA, the manufacturer will be exempted from product liability if it proves that the defect in the product could not have been discovered given the state of scientific or technical knowledge at the time the manufacturer delivered the product (PLA Article 4).

5.3 Cybersecurity and Data Protection

The number of cyber-attacks against the healthcare industry has increased significantly. The Japanese government has designated the healthcare industry as one of the 14 important sectors that require elaborate countermeasures to combat cyber-attacks swiftly and efficiently.

There is no specific legislation or rules governing cybersecurity issues concerning IoMT or connected devices malfunctions. However, the MHLW, the Ministry of Economy, Trade and Industry and the Ministry of Internal Affairs and Communications have introduced two guidelines on health information at large, namely:

- the Safety Management Guideline for Providers of Information Systems and Services that Handle Medical Information; and
- the Guideline on Safety Management of Medical Information Systems.

The latter provides guidance for medical institutions and applies to information created or recorded by healthcare providers.

The Guideline requires the preparation of the following:

- internal standard operating procedures for safety management;
- the establishment of committees for management and incident response;
- the implementation of staff training and incident reporting and responding standards; and
- measures to prevent eavesdropping, falsification or security breaches when exchanging information with outside parties via the network.

The Guideline also contains a specific checklist of cybersecurity measures that should be employed by medical institutions.

The Safety Management Guideline for Providers of Information Systems and Services that Handle Medical Information contains guidance for providers that supply medical information systems and resources and the services necessary for those medical information systems, and for providers that receive medical information from medical institutions based on the instructions of patients, including:

- providers of applications ("application service providers/service as software");
- platforms;
- infrastructure ("infrastructure as a service"); and
- communication lines ("Providers").

The Guideline sets out specific and detailed guidance on the recommended practices to be adopted by the Providers, such as measures against ransomware, and also requires Providers to obtain a privacy mark or an information security management system certificate. In addition, the Guideline provides detailed requirements regarding the risk management process (ie, risk assessment, risk analysis, risk management and risk communication) to be followed by the Providers.

5.4 Proposed Regulatory Developments

The Guideline on Safety Management of Medical Information Systems was updated in January 2021, and the Safety Management Guideline for Providers of Information Systems and Services that Handle Medical Information was updated in August 2020. Since then, there has been no notable change or proposed change in the regulations or guidance.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Legislation Framework

There is no specific legislation for the digital health sector, including software as a medical device (SaMD). Rather, existing legislative schemes apply to digital health products.

A product, which may be either a device or software, that constitutes a medical device is governed by the Pharmaceuticals Act. That Act defines a medical device as an instrument (including a computer program) that is intended for use in the diagnosis, treatment or prevention of disease in humans or animals, or is intended to affect the structure or function of human or animal bodies (excluding regenerative medicine products, which are separately regulated), and that is specified by a Cabinet Order.

If a company's digital health product constitutes a medical device, the company must obtain a marketing licence, manufacturing licence and distributing licence in order to conduct marketing, manufacturing and distribution of the device, as well as authorisation, certification or notification for the specific device, according to the statutory classification. This is determined in accordance with the risk that the device would injure the human body in the case of malfunction. The classification is harmonised through the International Medical Device Regulators Forum, which succeeded the Global Harmonisation Task Force founded by Japan, the USA, the EU, Canada and Australia.

More specifically, a Class I medical device is classified as a general medical device under the Pharmaceuticals Act and requires only notifica-

tion to the regulator. A Class II medical device is usually classified as a controlled medical device and requires a marketing authorisation from the PMDA, but certain categories of Class II medical devices designated as relatively low risk are exempt from the requirement for a marketing authorisation and require only certification by an accredited body. Similarly, Class III and Class IV medical devices are classified as specially controlled medical devices requiring a marketing authorisation from the PMDA, with a few exceptions (designated specially controlled medical devices) requiring only a certification by an accredited body.

The question of whether a clinical trial is required depends on the classification of the product, the difference between the product and existing products on the market and the possibility of establishing the efficacy and safety of the product by means other than a clinical trial. However, a medical device with an apparently different structure, usage, effect or performance from existing medical devices will most likely be subject to a clinical trial and application for authorisation from the PMDA, regardless of the aforementioned classification.

Software as a Medical Device

The MHLW and other governmental bodies have issued guidance regarding the digital health sector. Notably, the MHLW issued the Basic Concept on whether a Computer Program falls under the Medical Device, which provides a clearer indication than is provided in the Pharmaceuticals Act, and a ministry ordinance on whether certain software constitutes a medical device. The guideline states that the question of whether certain software constitutes a medical device should be decided based on the impact that the software has on the diagnosis and treatment of a disease, considering the significance of the results obtained by the software, and the risk of affecting the life and health of a person in the event of software malfunction. Even if certain software is used in the diagnosis, treatment or prevention of disease, it will not be treated as a medical device if it has a very low risk of injury to humans that is comparable with the risk of a Class I (hardware) medical device. Furthermore, the guideline contains examples of software that do and do not constitute medical devices.

The SaMD Guideline mentioned in **2.2 Recent Regulatory Developments** further distinguishes between various types of software according to their purpose and function, especially whether the software is to be used by medical professionals or by laypersons. Therefore, the purpose and function of the software must be clarified first. The Guideline then requires comparison between the purpose and function of the software with the purpose and function of existing software already categorised as a medical device. If the software has a similar purpose and function to those that are already categorised as a medical device, the software is also likely to be categorised as a medical device.

7. Telehealth

7.1 Role of Telehealth in Healthcare

Guidelines Regarding Online Medical Treatment

In Japan, telehealth is mainly discussed in the context of online medical treatment. Under the Guidelines for Appropriate Performance of Online Medical Treatment, dated March 2018 (amended in March 2023), the MHLW describes “matters to be complied with at minimum” and “matters recommended” with respect to online medical treatment in order to promote its appropriate use.

Article 20 of the Medical Practitioners' Act stipulates that "no medical practitioner shall provide medical treatment or issue a medical certificate or prescription without personally performing an examination". Thus, arguably, in the past, an online medical treatment might have violated Article 20. However, the above Guidelines clarified that an online medical treatment does not violate Article 20 if that treatment is performed in compliance with the "matters to be complied with at minimum" under the Guidelines.

Definition of Online Medical Treatment

Under the Guidelines, telemedicine is defined as "an act concerning health improvement and medical treatment using information communications equipment". Also, online medical treatment is defined as "a type of telemedicine, which is an act of medical treatment, such as carrying out examinations, making diagnoses, transmitting examination results and prescribing medicines in real time by using information communications equipment".

Matters to Be Complied With at Minimum

The Guidelines describe the "matters to be complied with "at minimum", which include, among others, the following:

- a doctor and a patient must agree to the performance of an online medical treatment;
- in principle, online medical treatment from the first medical examination must be conducted by a primary care doctor;
- a doctor must prepare a medical treatment plan based on the result of the face-to-face medical examination and maintain that plan for two years;
- in principle, the identity of the doctor and patient must be verified through identity-verification documents;
- a prescription for certain pharmaceuticals must not be issued at the first medical examination; and
- an online medical treatment should be conducted using information communication tools with real-time visual and auditory information in order to obtain as much medical information as possible.

Regulation Regarding Online Medication Counselling

Another development of telehealth in Japan is online medication counselling.

Formerly, the Pharmaceuticals Act stipulated that medication counselling must be conducted face to face.

However, the Pharmaceuticals Act was amended in September 2020 to allow online medication counselling under certain conditions.

The conditions for online medication counselling are as follows:

- medication counselling was previously conducted face to face;
- online medication counselling should be conducted using a medication instruction plan that describes certain matters; and
- pharmaceuticals to be sold or given away must be prepared using a prescription issued by an online medical treatment or home-visit medical treatment.

7.2 Regulatory Environment

Temporary Relaxation of Regulations

Due to the spread of COVID-19, the MHLW issued a notice on 10 April 2020 temporarily relaxing regulations regarding online medical treatment and online medication counselling.

Relaxation of Regulations Regarding Online Medical Treatment

Physicians were permitted to conduct a patient's initial medical examination using online medical treatment if the doctor determined that it is medically possible to make diagnoses or prescribe medicines through a medical examination using a telephone or information communications equipment. However, a doctor must attempt to gather and confirm information regarding a patient through past medical records, the medical information provision form, a local medical information collaboration network or a medical examination result.

Also, in order to conduct the initial medical examination by telephone or information communications equipment, the following conditions must be satisfied:

- a doctor must provide a patient with sufficient information (such as regards possible risks, policy in the case of emergencies, etc) and must record the content of the explanation in the patient's medical records;
- a doctor must secure a system for switching smoothly to face-to-face medical treatment if necessary; and
- a doctor must verify a patient's identity and eligibility.

Furthermore, a medical institution must report the implementation status of online medical treatment on a monthly basis to the prefecture in which the medical institution is located.

Relaxation of Regulations Regarding Online Medication Counselling

Pharmacists were permitted to conduct online medication counselling if the pharmacist determined that it is possible to conduct medication counselling appropriately by telephone or information communications equipment, based on information regarding the patient and their medication status.

Also, in order to conduct medication counselling by telephone or information communications equipment, the following conditions must be satisfied:

- a pharmacist must provide a patient with sufficient information (such as regards possible risks, procedure of delivery and confirmation of medication status), and must record the content of the explanation;
- a pharmacist must confirm medication status and side effects by telephone during the medication period for a drug prescribed for the first time, in order to encourage medication adherence and secure appropriate usage of a drug;
- a pharmacist must switch smoothly to face-to-face medication counselling if necessary; and
- a pharmacist must verify a patient's identity and eligibility.

7.3 Payment and Reimbursement

In Japan, payment by a patient for medical treatment at a medical institution is generally covered by national health insurance and a patient is required to pay only a portion of the cost of medical treatment at a medical institution.

Also, medical fees for medical treatment are prescribed by the MHLW.

Medical fees for online medical treatment and online medication counselling are also prescribed by the MHLW; therefore, insurance reimbursement is available for a patient who receives online medical treatment and online medication counselling.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

The IoMT makes it possible for various and multiple smart devices, including wearables and implantables, to connect with each other through the internet. 5G networks, which have been available in Japan on a limited commercial basis since March 2020, enable high-speed data exchange with other devices and hospital networks. The large volume of data to be collected through the networks is useful for AI to study.

Concerning the security risks associated with use of the networks, such as use of a cloud storage service for storing electronic medical records and images, the MHLW issued the Guidelines regarding Security Management of Medical Information Systems, with which medical institutions must comply. Additionally, the Ministry of Internal Affairs and Communications (MIAC) and the Ministry of Economy, Trade and Industry jointly issued the Security Management Guidelines for Information System Service Providers dealing with Medical Information, with which service providers must comply. The Guidelines appear to take a risk-based approach – ie, requiring the parties to:

- identify the risks;
- analyse the level of each risk;
- evaluate how to treat the risk, based on the analysed level of each risk;
- treat the risk, evaluate the remaining risks and the record thereof;
- reach an agreement; and
- continue risk management.

Various types of digital assistants for human health have been introduced recently. To the extent that certain digital assistants fall within the scope of medical devices to be regulated by the Pharmaceuticals Act, the digital assistants would be subject to the same regulations. Whether the digital assistants fall within the scope of medical devices depends on the importance of the results to be generated by them and the seriousness of the risk that may be caused by a malfunction or defect in the digital assistant. For example, in 2020, the PMDA approved, as regulated medical devices:

- a program for curing nicotine addiction; and
- Apple's electrocardiograph program and heart-rate monitoring program for Apple Watch.

By contrast, the MHLW found that a tool for predicting the onset of diabetes, which was uploaded for the public by the National Centre for Global Health and Medicine on its website in 2018, did not fall within the scope of regulated medical devices. A program that takes an important role in a doctor's diagnosis of diabetes would appear to be a medical device, while a program that only shows the possibility of developing diabetes in the near future would not be considered a medical device.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

5G networks are wireless telecommunications networks with high speed, large capacity, low latency and multiple connections. They are expected to enable telemedicine, remote surgery, online medication instruction and online collection, storage and use of medical data and images. These are especially valuable for medical treatment in disaster areas. 5G networks

are also considered to be able to mitigate the reduced access to medical treatment of residents, including elderly people, in rural areas that may be caused by the uneven distribution of doctors in urban and rural areas in Japan.

However, the areas in which 5G networks are available are still limited. Further, when healthcare institutions enter into arrangements with telecommunications providers to deploy and manage 5G networks, those institutions must address the allocation of the risks that may arise, such as interruption, malfunction and defects of the networks. Similarly, allocation of the risk of potential infringement of intellectual property rights owned by third parties may also be an issue.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

Law to Protect Data Relevant to Personal Health

The APPI provides protection for personal data handled by private entities. While the APPI does not provide a special protection and management scheme for data relevant to personal health, it defines "special care-required personal information" as personal information that may lead to discrimination against, or other disadvantage to, an individual, such as information regarding race, religion, social status, medical records and criminal records. Therefore, data relevant to personal health usually falls within the definition of special care-required personal information.

Disclosure of Personal Data to a Third Party

Under the APPI, disclosure of personal information to a third party requires consent from the data subject. Consent may be obtained through an opt-out procedure. Pursuant to an opt-out procedure, disclosure of personal information to a third party will be permitted without the individual's explicit consent if the individual was informed (or was otherwise notified in a way that made it possible for the individual to acknowledge) that their personal information would be disclosed to a third party, and the individual had the opportunity to refuse disclosure.

However, an opt-out procedure is not permitted for the disclosure of special care-required personal information. Therefore, explicit consent must be obtained prior to providing health data to third parties if that health data is considered to be special care-required personal information.

Anonymisation of Data

The APPI defines the term "anonymously processed information" as information relating to an individual that may be created by processing personal information so as not to be able to identify a specific individual. In particular, processing personal information for de-identification means deleting:

- descriptions that may identify a specific individual;
- individual identification codes;
- codes that link the processed information with the personal information; and
- idiosyncratic descriptions (ie, descriptions that could identify an individual because of the uniqueness of the information).

The APPI substantially eases the restrictions on the acquisition, disclosure and use of personal

information for anonymously processed information.

However, explicit consent is still required when providing special care-required personal information to an outside information processor for the anonymising process. Moreover, medical information is often held by individual hospitals and entities, and explicit consent from the patient is required when the original data, which in many cases constitutes special care-required personal information, is provided to, or used by, an outside information processor. Therefore, the accumulation of medical information and construction of a database has been difficult.

To ease this difficulty, Japan has enacted the Act Regarding Anonymised Medical Data to Contribute to R&D in the Medical Field (the "Next-Generation Medical Infrastructure Act", or NGHIA) to facilitate the accumulation of medical information and to promote the use of big data for the development of medical technologies, while also protecting patients' privacy and personal information. Under the NGHIA, the Japanese government authority will examine and authorise entities to be data-processing entities that collect, de-identify and provide medical information to third parties (Authorised De-identified Medical Information Preparer). Provision of medical data to the Authorised De-identified Medical Information Preparer still requires consent from the patient, but the opt-out procedure applies. The Authorised De-identified Medical Information Preparer will identify and link a patient's data from different medical institutions, adjust the data format and integrate the data into a database. When a third party, typically a healthcare company or a research institution, requests data, the Authorised De-identified Medical Information Preparer will select the relevant data, de-identify it and provide an anonymised data set for a fee.

Enforcement

Under the APPI, the Personal Information Protection Commission, an organisation within the Cabinet Office, provides the necessary guidance and advice to business operators handling personal information, including health data, and collects reports, conducts on-site inspections and makes recommendations and orders regarding legal violations. Japan does not have a long history of using digital healthcare technology, so no notable regulatory or private enforcement actions have yet been published in the medical service sector.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

AI and Medical Devices

Artificial intelligence (AI) technology has been developed in recent years and has the potential to design programs with performance that would have been difficult to achieve with conventional algorithms, such as enabling detailed prediction of disease changes in patients and detecting lesions that even a specialist could not identify.

The question of whether a specific AI program should constitute a medical device (and therefore be subject to the Pharmaceuticals Act) is determined based on the same concepts as other programs using conventional algorithms. However, the relationship of AI technology-based programs to medical devices must be considered in connection with the specific risks associated with the level of technology at the time, such as how to add new data for machine learning.

In accordance with the Pharmaceuticals Act, the term "programmed medical device" means

programs intended to be used for diagnosis, treatment or prevention of human diseases in the form of tangible objects installed in general-purpose computers, personal digital assistants, or to influence the structure or function of human bodies. However, programs that are unlikely to have an impact on human life and health, even if functional impairment occurs, are excluded from the scope of medical devices.

The following programs using AI technologies will be included in the scope of medical devices:

- a program in which AI substitutes for diagnoses that can only be performed by specialists, such as detecting cancer with a certain degree of accuracy and predicting life expectancy using medical images;
- a program in which AI predicts the name of a disease based on information such as body temperature and blood pressure entered by non-healthcare professionals using an original algorithm; and
- a program that uses AI to identify and assist in the testing of suspected disease areas during the use of a medical device.

By contrast, the following programs will be excluded from the scope of medical devices:

- a program that allows users to enter health data and self-manage their weight and health based on information provided by AI;
- a program that provides detailed 3D images of the human body after image correction by AI for use in medical students' learning and in patient explanation;
- a program in which AI extracts necessary information from medical record information and presents the names of potential diseases along with the relevant parts of the guidelines and the basis for the determination according to information on publicly available medical care guidelines;
- a program utilising AI that presents the information necessary for medical practice from clinical data using publicly available formulas;
- a program that uses AI to allow doctors to search for publicly available guidelines and package inserts when making a diagnosis; and
- a program using AI that assists in the use of medical devices in accordance with known guidelines.

Cybersecurity

For details on AI and cybersecurity, see **5.3 Cybersecurity and Data Protection**.

11.2 AI and Machine Learning Data Under Privacy Regulations

The MHLW published Benchmarks for Next Generation Medical Device Evaluation on 23 May 2019. It included Benchmarks for Evaluation of Medical Image Diagnosis Support Systems Using Artificial Intelligence Technology. It provided the MHLW's view on points to be considered when evaluating the effectiveness and safety of medical image diagnosis support systems using AI technology.

In December 2019, the Ministry of Economy, Trade and Industry (METI) also published Guidelines for the Development of Medical Diagnostic Imaging Support Systems (Including Systems Using Artificial Intelligence Technology), which summarises the points to be considered by researchers and developers during the development of Computer Aided Diagnosis (CAD) systems. These Guidelines are a revision of the developmental guideline on CAD published in the early 2010s and combine the then two existing CAD development guidelines into one, with an additional description on AI technology.

Under the APPI, medical information is further classified into special care-required personal information, for which care must be taken when handling such information. In addition, it is necessary to obtain the consent of patients when handling such information outside medical institutions. It is also necessary to obtain consent for the intended use, such as for the learning of AI in medical devices and applying the learning results to products. In the case of academic research, personal information may be used for research without individual consent under Article 76 of the APPI. However, this Article does not apply in cases of product development. On the other hand, the use of medical information in academic research is highly likely to fall under "clinical research" stipulated in the Clinical Research Act or "research" stipulated in the Ethical Guidelines for Life Science and Medical Research Involving Human Subjects, and the consent of the research subjects is required. The collection, use and storage of data based on clinical trials under the Pharmaceuticals Act need to comply with GCP Ordinances set forth by the MHLW and are not subject to the APPI.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Established IT companies have vast experience and resources for dealing with personal information through existing businesses, but they still need to pay close attention to regulations under the Personal Information Protection Act because the information dealt with by digital healthcare technology is highly sensitive, and personal information and the Personal Information Protection Act itself (and the ordinances and guidelines thereof) have been updated. Healthcare institutions and other clients need to make sure that their agreements with vendors manage their personal information properly. Further, it is necessary to comply with the regulations under the Pharmaceuticals Act, which is usually new to such companies. Such regulations have traditionally been handled by in-house specialists in pharmaceutical and medical device companies. Some established IT companies have started to hire regulatory specialists as well as to seek consultation with independent external experts on the matter.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

Japan is the first country in the world to have a rapidly declining birth rate and an ageing population. Under these circumstances, it is necessary to take measures to promote a healthy life expectancy of each citizen, and to ensure the sustainability of social security. Such measures include improving efficiency and productivity, while also maintaining and improving the quality of services at busy medical and nursing sites.

These issues must be addressed by:

- promoting ICT in the fields of health, medical care and nursing care;
- ensuring that each and every citizen and patient makes effective use of their own medical and other data; and
- enuring that health and medical facilities and related industries make appropriate use of that data.

Social Changes, Data Protection and Cybersecurity

In addition, the social change known as Society 5.0 is rapidly progressing, through the use of advanced information and communication

technologies and data. In the field of healthcare, data is handled not only by entities engaged in healthcare, but also by new entities, including private companies. These social changes have brought about a number of important issues that must be addressed, not only in Japan but also internationally, such as rules for data utilisation, the protection of personal information, and cybersecurity measures.

Special consideration should also be given to privacy regarding health, medical and nursing care information. For this reason, all actors, including the State, must take necessary measures in promoting these efforts. In particular, it is essential to take all possible measures to ensure information security in the medical field, as one of the important infrastructure fields.

With the advancement of ICT in the medical field, it is also important to confirm the identity of healthcare workers and promote measures to prevent forgery and falsification of electronic documents.

Information Management

From the viewpoint of the availability of user data stored in cloud services, public entities that use cloud services to collect and store medical and other information nationwide must be required to:

- ensure thorough information management by selecting domestic data centres subject to Japanese laws;
- conclude treaties and cloud services with jurisdiction over Japan as candidates for adoption; and
- make cloud security certification mandatory.

Medical information is also subject to the APPI as personal information requiring special care. However, from the perspective of protecting medical information while also promoting the use of information and the promotion of research and development at medical sites, issues remain, such as how to obtain consent from individuals.

The Japanese government plans to examine the handling of personal information in the medical field while investigating the status of legislation in foreign countries regarding the protection of personal information (including issues related to data portability) in the medical field.

13.2 Data Management and Regulatory Impact

In August 2020, METI and MIAC issued the Safety Management Guidelines for Providers of Information Systems and Services Handling Medical Information, which combines two sets of then-existing guidelines (ie, the Safety Management Guidelines for Information Processing Service Companies Managing Medical Information issued by METI, and the Guidelines for Safety Management by Cloud Service Providers Handling Medical Information issued by MIAC). The purposes of the combined Guidelines are to:

- ensure the same level of safety management as compliance with past guidelines, while taking into account consistency with other standards and guidelines;
- define risk management processes based on a risk-based approach for the purpose of designing necessary and sufficient measures according to the characteristics of medical information systems, etc;
- emphasise risk communication for the purpose of operating medical information systems, etc based on a correct common understanding and explicit agreement on the efficacy and limitations of security measures; and

- clarify points to be considered in the handling of medical information and requirements in the system for the purpose of preventing omission of required measures under the laws and regulations related to medical information systems.

In March 2022, the MHLW issued Guidelines for the Safety Management of Medical Information Systems, Version 5.2, which describe, from the viewpoint of technical and operational management, necessary measures for ensuring the safety management of medical information systems and appropriate compliance with the Act on the Utilisation of Information and Communications Technology in Document Preservation Conducted by Private Business Operators, etc. Section 6.8 "Modification and Maintenance of Medical Information Systems" of the Guidelines states that regular maintenance is necessary to maintain the availability of medical information systems. Such maintenance work includes troubleshooting, preventative maintenance and software revision. As the system maintenance personnel may have direct access to medical information in administrator mode, the Guidelines require sufficient countermeasures against possible data leakage.

14. Intellectual Property

14.1 Scope of Protection

Hardware can be protected by a patent, utility model right or design right, provided that:

- the hardware is novel; and
- it has an inventive step over prior art or is not similar to prior designs.

Software is eligible for protection not only by copyright, but also by patent and utility model right, and may also be protected as a trade secret. User interfaces for medical devices may be protected by copyright and design right. Notwithstanding the foregoing, methods for medical treatment are not eligible for protection by patent or utility model right.

Data and databases used in machine learning are eligible for trade secret protection, provided that confidentiality can be maintained. Big data, which is not managed in such a way as to maintain confidentiality but is collected and managed to be provided to other specified entities, may also be protected under the Unfair Competition Prevention Act. A database is also eligible for copyright protection as long as it is creative in terms of selection or systematic construction of data contained therein.

Despite recent frequent discussions, there is no prevailing view under Japanese law regarding inventions and works of authorship created by AI technologies without direct human contributions. However, a person or entity operating AI technologies with a certain purpose or theme may be recognised as an inventor or author.

14.2 Advantages and Disadvantages of Protections

Patents for inventions which are claimed as consisting of elements accessible by users and design rights in user interfaces are good in the sense that it is easy to identify the infringement carried out by competitors, whereas structures and codes that are embedded in competitors' programs and data are difficult to identify. Further, patents and design rights are easier to enforce in many cases compared to copyright or trade secrets because alleged infringers' access to or knowledge of such rights are not required as a condition for enforcement thereof; whereas alleged infringers' access to, or knowledge of,

the original works or the trade secrets which have been managed to be kept secret is required as a condition for enforcement thereof.

That said, the life of patents and design rights is limited to 20 or 25 years from filing, while copyright protection is eligible for 70 years and there is no periodical limitation for trade secret protection. Further, patents and design rights are easy to design around, whereas eliminating contamination of copyrighted codes or trade secrets is not so easy. Therefore, it is important to protect products or processes by a combination of multiple types of intellectual properties.

14.3 Licensing Structures

There are various types of licensing structures in this field but, in some cases, it is preferable for intellectual property (IP) holders to charge a running fee on a monthly or yearly basis rather than receiving a lump sum payment. In such cases, it is necessary to be careful that patents and design rights can be subject to exhaustion of rights once products protected by such rights are sold by holders or licensees thereof. A combination of granting a licence of software and data as well as providing support for updating it can be legitimate grounds for claiming a running fee.

14.4 Research in Academic Institutions

As long as university or healthcare institutions ("Institutions") have their own rules stipulating that they acquire IP rights over inventions, etc, created by physicians/inventors working for the Institutions in the course of performing their tasks, the Institutions will own the rights to file applications for patents, utility model rights and design rights. However, the physicians/inventors are eligible for reasonable compensation. Additionally, the Institutions will be recognised as authors and holders of trade secrets and big data.

If IP is jointly created by two entities, such as by a university and a private company through their joint research and development, the IP rights will be jointly owned by those entities unless otherwise stipulated in the governing agreement. If patents, utility model rights or design rights are jointly owned by multiple parties, each party may exploit those inventions without consent from the other parties, although assignment and licensing will require consent, unless otherwise stipulated in the governing agreement. Copyrighted works may not be used, assigned or licensed without consent of the other joint owners, unless otherwise stipulated in the governing agreement.

14.5 Contracts and Collaborative Developments

It is most desirable to have all joint ownership assigned to a single entity subject to its control. In such a case, the right to create derivative works and the right of the original author over derivative works under Articles 27 and 28 of the Copyright Act of Japan must be expressly stipulated as included in the assigned rights. Further, as the moral rights of authors are not assignable, authors must promise not to exercise those rights. If the rights are to be jointly owned by multiple parties, a contractual provision should address the exploitation of rights by a single joint owner.

15. Liability

15.1 Patient Care

In Japan, final decisions on diagnosis and medical treatment must be made by doctors, regardless of whether the doctors are using healthcare technologies such as data analytics or medical

devices driven by AI or software. Accordingly, in principle, doctors and the medical institutions for which they work are considered to be responsible for the diagnosis or medical treatment and also liable for any injury caused to their patients thereby. However, both civil and criminal liability of doctors and medical institutions require a showing of physician negligence, and the burden of proof is on the patient. A doctor's reliance on digital assistance through healthcare technology is not an absolute defence, but in such a case, an accuser would be required to establish the doctor's negligence in the selection, maintenance or operation of the device.

If a doctor is successful in proving the possibility of malfunction or latent defects in the medical device, the doctor and relevant medical institution may not be found liable. There is no special legislation under which doctors and medical institutions are immune from liability, or are subject to strict liability, simply because the doctor relied on healthcare technology. Bias in AI or the possibility or failure of recognition thereof are factors that may affect a finding of negligence.

15.2 Commercial

Healthcare institutions that entered into contracts with vendors may choose to pursue contract claims against those vendors. A healthcare institution seeking to bring a contract claim against a vendor would be required to establish that:

- the vendor's products or services did not comply with the specifications or service level of the products or services agreed between the institution and the vendor;
- the vendor was negligent with respect to that non-compliance; and
- the damages caused to the healthcare institution by the vendor's products or services were foreseeable by the vendor.

For claims of healthcare institutions against vendors which are not parties to a contract with those institutions, contract claims are not available. A tort claim may be an option, provided, however, that those institutions have the burden to prove vendors' negligence or wilful misconduct and predictability of causing the damages.

Further, healthcare institutions may bring a claim under the Product Liability Act, which prescribes manufacturers' strict liability for damages caused by product defects. The term "defect" as used in this Act means a lack of safety that the product ordinarily should provide, taking into account:

- the nature of the product;
- the ordinarily foreseeable manner of use of the product;
- the time when the manufacturer delivered the product; and
- other circumstances concerning the product.

Trends and Developments

Contributed by:
Yoshiyuki Inaba, Satoshi Ogawa, Hitoshi Fujimaki and Suguru Saito
TMI Associates

TMI Associates was established on 1 October 1990 and has grown rapidly to become a full-service law firm that offers comprehensive legal services of the highest quality. TMI Associates provides support in the digital health and life sciences field. The firm's healthcare practice group has supported a wide range of clients, including domestic and global healthcare start-ups, universities, pharmaceutical and medical device companies, venture capital and governmental organisations. TMI is proactively engaged in all aspects of the field, such as advising on pharmaceutical regulations, IP acquisition and utilisation, conducting legal and IP due diligence for M&A and IPO, drafting and negotiating licence agreements and assisting patent litigations. The firm is in close contact with the Ministry of Health, Labour and Welfare, to which its attorneys have been seconded. TMI Associates examines risks based on its precise grasp of the practical operation and interpretation of relevant regulations and guidelines in the field.

Authors

Yoshiyuki Inaba is a senior partner of TMI Associates and has more than 45 years' experience. He heads the intellectual property group, utilising his expertise in patent and trade mark prosecutions and enforcement to oversee the daily management of each client's IP portfolio, ensuring that proper protection is obtained and that the client's interests are fully covered. He also handles and supervises patent and trade mark lawsuits at both the District and IP High Court levels, as well as conducts invalidation procedures at the Japan Patent Office. In addition, he is active in negotiations for clients, including those regarding licensing, transfers and general co-operative arrangements.

Satoshi Ogawa is a partner at TMI Associates whose expertise is in all aspects of the life science and healthcare fields. He is mainly involved in IP licensing, regulatory works, conducting IP due diligence for IPOs, and M&A. Satoshi earned a PhD in life sciences, and based on his knowledge of cutting-edge technology, such as regenerative medicine, iPS cells and genome editing, he has represented a wide variety of foreign and domestic clients in these fields. Having worked at an Indian law firm for some years, he has vast experience of India–Japan-related work.

Contributed by: Yoshiyuki Inaba, Satoshi Ogawa, Hitoshi Fujimaki and Suguru Saito, **TMI Associates**

Hitoshi Fujimaki is an associate attorney at TMI Associates who focuses his practice primarily on healthcare law, including the regulation of digital health matters, such as medical device programs, telemedicine and online medication guidance. He is a leading member of the healthcare practice group at the firm. Hitoshi earned his LLM degree in National and Global Health Law with a Food and Drug Law Certificate from the Georgetown University Law Center. He worked for four years as a member of the legal affairs team of the Tokyo Organising Committee of the Olympic and Paralympic Games Organization for the 2020 Tokyo Olympic and Paralympic Games.

Suguru Saito is an associate attorney at TMI Associates with particular expertise in patent law, space law and healthcare law, including the regulation of digital health issues and healthcare-related IP transactions. He is a member of the firm's patent practice group, aerospace practice group and healthcare practice group.

TMI Associates

7th Floor Yoshichu Building
525 Wataya-cho
Nakagyo-ku,
Kyoto-shi
Kyoto 604-8181
Japan

Tel: +81 75 256 5531
Fax: +81 75 256 5588
Email: sogawa@tmi.gr.jp
Web: www.tmi.gr.jp

TMI Associates

General

Currently in Japan, people aged 65 years and older make up approximately 30% of the population. Japan's ageing population is unprecedented and poses serious societal problems, such as a relatively decreasing labour force and increasing social security costs. In recent years, there have been moves towards resolving these problems using technologies such as artificial intelligence (AI) and the internet of things (IoT). As a result, new businesses and start-ups have emerged that are creating new technologies and services in this area.

These developments were intensified because of the COVID-19 pandemic. As in other countries, since 2020 remote working and non-contact activities have become routine in Japan and, therefore, the practical application of digital health technologies has been accelerating. In addition, the ruling Liberal Democratic Party (LDP) and the Japanese government announced policies aimed at promoting Digital Transformation (DX) in the medical field in 2022.

Progress was made in 2022 in various digital health areas, such as the expansion of remote medical care, the increase in healthcare-related apps, and the utilisation of healthcare data and the metaverse.

Government Policies

In May 2022, the LDP released their proposal for the "Medical DX Reiwa Vision 2030", and in June 2022, partly based on such proposal, the Cabinet adopted the "Basic Policy on Economic and Fiscal Management and Reform 2022". This basic policy defines the goals regarding medical DX in Japan and states that "[w]e will optimise medical and long-term care costs, pursue quality visualisation and innovation based on the certification system and evaluation guidelines for relevant services aimed at revitalising digital health to improve the efficiency and quality of services through DX and other technological innovation in the medical and long-term care fields, and at the same time we will steadily implement reforms such as pursuing PHR in accordance with the Data-based Health Management Initiatives Roadmap. The government and relevant industries will work together to establish a national medical information platform, standardise electronic medical record information, and apply DX to the revision of medical service fees, and take legislative measures on the use of medical information."

In addition, the Ministry of Health, Labour and Welfare (MHLW) established a special promotion team for the "Medical DX Reiwa Vision 2030" in September 2022, and the Cabinet Secretariat established the "Medical DX Promotion Headquarters" in October 2022 in order to achieve such goals. In April 2023, the LDP released "Towards the Realisation of the Medical DX Reiwa Vision 2030: a Country Where All Citizens Can Receive Optimal Healthcare through the Digital Use of Health and Medical Information", which proposed policies for the implementation of the "Medical DX Reiwa Vision 2030", including:

- the grand design;
- the strengthening of governance;
- the national medical information platform; and
- the standardisation of electronic medical record information.

Expansion of Remote Medical Care

Background

Previously in Japan, medical services were administered face-to-face. Remote medical care was regarded as a supplement to face-to-face treatment and its use was limited. Face-to-face

guidance on the administration of medication had been mandatory. However, in recent years, in addition to the development of information and communication devices, there has been a temporary relaxation of related regulations as a response to the increased demand for online medical treatment and online medication guidance during the COVID-19 pandemic. This has resulted in the widespread use of telemedicine and online medication guidance.

Telemedicine

The limitations of Japanese telemedicine have been discussed for some time in relation to Article 20 of the Medical Practitioners' Act, which prohibits physicians from providing medical treatment without an examination. In this context, the MHLW formulated the Telemedicine Guidelines in March 2018, stipulating the minimum compliance requirements for telemedicine and clearly stating that compliance with the Guidelines does not violate Article 20 of the Medical Practitioners' Act.

These Guidelines specify that an initial medical consultation is to be conducted in person, which did not necessarily lead to the expansion of its use. However, the MHLW revised the Guidelines in January 2022 in response to the increased use of telemedicine during the COVID-19 pandemic. It widely approved the use of telemedicine from the initial treatment, even with the pandemic coming to an end. In addition, the MHLW revised the Telemedicine Guidelines in March 2023 and provided additional guidelines, such as personal identification and security for the telemedicine system.

According to the Telemedicine Guidelines, telemedicine from the first examination is permitted in the following cases:

- when the first examination is conducted by a "family physician" (a physician who has an existing direct relationship with the patient, such as one who has been regularly and directly treating the patient);
- when medical information, such as the medical history, is available and the physician determines it possible to provide telemedicine, in accordance with the patient's symptoms; and
- when a physician consults a patient before treatment (ie, when a physician checks the patient's symptoms and medical information before formal medical treatment) in cases where the family physician is absent or in other specific situations.

However, according to the Telemedicine Guidelines, there are certain limitations, such as when symptoms are not suitable for an initial treatment by telemedicine or when certain medicine is prohibited from being prescribed at an initial examination. In addition, medical treatment solely by telephone or by an exchange of letters or documents is not permitted. Moreover, telemedicine requires information and communication methods that include both visual and auditory information.

Japan has a universal health insurance system that allows all residents to receive insured medical care at a low cost. Previously, there were only a limited number of diseases that could be treated by telemedicine that were covered by insurance, and medical fees were lower than those for face-to-face treatment. However, with the revision of medical fees in 2022, limitations on the number of diseases that could be treated were eased, and medical fees became almost the same as those for face-to-face treatment. It is expected, therefore, that there will be an increased use of telemedicine in the future.

Telemedicine itself can only be provided by a physician, but in cases where the content of the advice does not include medical judgement, such advice may be given by a person who is not a physician without the application of the Medical Practitioners' Act and the Telemedicine Guidelines. Such health consulting services are positioned as a preliminary step to telemedicine. They remain in high demand for helping with the early detection of diseases, and there are low barriers to entry into the business.

Moreover, the Telemedicine Guidelines allow telesurgery in which a highly skilled physician operates on patients with separate physicians at a distant place using information and communication devices under certain conditions. This telesurgery makes it possible for physicians in remote areas to provide medical care that takes advantage of the specialised knowledge and skills of such physicians. The Telemedicine Guidelines also state that telesurgery must be implemented in accordance with certain guidelines by the respective associations, etc which determine the detailed coverage, such as specific target diseases and patient conditions. In June 2022, the Japan Surgical Society published their telesurgery guidelines, which have resulted in various forms of collaborative research and the further development of telesurgery in Japan.

Online medication guidance

In Japan, the separation of medical and dispensary practices has been adopted. Under this system, physicians prescribe drugs and pharmacists dispense the prescribed drugs and sell them to patients. Prior to the revision of the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices (the "Pharmaceutical and Medical Device Act") in 2020, the proprietor of a pharmacy had to provide face-to-face guidance by a pharmacist when selling or giving drugs prescribed by a physician so that the patient could be instructed in the proper use of the drugs.

While the revision of the Pharmaceutical and Medical Device Act made it possible to provide online medication guidance, it did not become popular as there were many restrictions, such as guidance only being allowed for prescriptions provided for telemedicine or home-visit medical care. However, in response to the high demand for online medication guidance during the COVID-19 pandemic, the Ordinance for Enforcement of the Pharmaceutical and Medical Device Act was revised. From April 2022, the cases for which online medication guidance can be provided have been expanded, so that:

- online medication guidance is available at first-time treatment;
- online medication guidance is available for all prescriptions and is not limited to prescriptions issued during telemedicine or home visits; and
- in addition to the drugs previously prescribed, online medication guidance is available for all drugs, in principle.

However, telemedicine requires video and audio communication, and voice-only (telephone) support is not permitted.

Example of a telemedicine system

Recently, the number of companies offering telemedicine systems has increased in Japan. For example, Medley, Inc provides the "Clinics Telemedicine System", Japan's largest telemedicine system in the medical platform sector. One of its applications allows for online appointments, prediagnostic interviews, video chat examinations, medication guidance, credit card payments, and drug/prescription delivery all at once, allowing

patients to continue receiving treatment without leaving their homes. This reduces the burden of outpatient visits, improves the rate of continuing treatments and prevents secondary infections at hospitals. LINE Healthcare Corporation also provides a telemedicine system using LINE, the most popular messaging application in Japan.

It is expected that online medical services, in conjunction with the provision of test kits and image analysis systems, will increase in the future.

Increase in Healthcare-Related Apps

Background

In 2020, a therapeutic app made by Cure App, Inc was approved as a medical device program for the first time in Japan. This app is designed to help nicotine-dependent patients stop smoking, and is covered by insurance. Since then, the number of applications for pharmaceutical approval of therapeutic apps has been increasing. Moreover, although there is a functional overlap with therapeutic apps, the development of recording apps, which are provided as a preparatory stage for the development of therapeutic apps, is rapidly increasing as, under the Pharmaceutical and Medical Device Act, licences and approvals are not required.

Therapeutic apps and symptom-recording apps

Therapeutic apps are used for the "treatment" of a specific disease in a medical setting and may be circumscribed by the following:

- as "medical device programs", they must be developed, manufactured and sold in accordance with the Pharmaceutical and Medical Device Act;
- approval to manufacture and sell them in Japan as new medical devices must be acquired from the MHLW after clinical trials have been conducted, which can take several years and be costly; and
- as a long period of time is required until the apps are covered by insurance, it can take considerable time and money until they reach the market.

Symptom-recording apps are used for "managing the health condition" of a healthy person and "recording symptoms" of a patient. A typical app is one that is used for recording health information, such as weight and blood pressure, daily. Their characteristics are as follows:

- they cannot express the therapeutic effects of the disease;
- since they are not "medical device programs", procedures based on the Pharmaceutical and Medical Device Act are not required; and
- their price can be freely set since they are not covered by insurance.

Such "medical device programs" are programs (software functions) that are intended to diagnose, treat or prevent diseases and are likely to affect a person's health in the event of a malfunction. Their manufacture and sale is regulated by procedures based on the Pharmaceutical and Medical Device Act. Therefore, even if they are defined as symptom-recording apps, they may correspond to medical device programs, depending on their functions and their proposed effects. It will be necessary to confirm whether such apps correspond to medical device programs when they are provided.

Since the criteria for determining whether a program is a medical device program was unclear, in March 2021 the MHLW established guidelines on the applicability of the term "medical device" to a program. According to these guidelines, it

is highly likely that a program corresponds to a medical device program in the following cases:

- where the diagnosis, treatment or prevention of disease is intended;
- where the candidate diseases and risk of disease are displayed based on input information; or
- where the program corresponds to Class II or higher when judged based on the Global Harmonization Task Force rules.

In recent years, many companies have been providing symptom-recording apps as a preparatory stage for the development of therapeutic apps, but sufficient attention must be paid to whether they can be defined as medical device programs.

Example of a therapeutic app

In addition to the above-mentioned smoking cessation application, Cure App, Inc received pharmaceutical approval for a therapeutic app for hypertension (accepted name: Hypertension Treatment Assistance Program) in April 2022. This is the first case in Japan in which pharmaceutical approval was obtained for the software itself, and it is the world's first pharmaceutical approval for a therapeutic app in the field of hypertension. The company is aiming to accomplish digital therapies that support improving lifestyles through apps for hypertension, rather than relying solely on drugs, and the app was launched in and has been covered by insurance since 2022.

It is expected that various therapeutic apps and symptom-recording apps will be introduced in the Japanese market in the future.

Utilisation of Healthcare Data

Background

In recent years, with the improvement of individual health awareness, the collection and use of information (healthcare data) – such as personal health status and medication records, including medical treatment, examinations, prescription, vital physiological data (eg, walking rates and pulse rates) – obtained by a wearable device and clinical trial data have been widely practised.

As this is a global trend, personal data is frequently transferred overseas, creating a variety of businesses in this area. Accordingly, the Act on the Protection of Personal Information of Japan was amended and came into effect in April 2022 (the "revised Act on the Protection of Personal Information") in order to respond to the increased need for the protection of personal information and the utilisation of personal information across borders.

Healthcare data and the revised Act on the Protection of Personal Information

Under the Act on the Protection of Personal Information, "special care-required personal information" is defined as information based on medical history, results of medical examinations, and the fact that guidance on medical treatment or dispensing of medicine has been provided based on such results. It is necessary to obtain the individual's consent for the use of such data.

In addition, regardless of whether or not such information is special care-required personal information, it is necessary to obtain the consent of the individual when providing such personal data to a third party; in particular, when the third party is located in a foreign country. In cases where personal data is provided through entrustment, the consent of the individual must

be obtained before the overseas transfer of such data.

Although the above regulations have been in force, the revised Act on the Protection of Personal Information requires that when obtaining consent from the individual for the overseas transfer of personal data, information concerning the system for the protection of personal information in the recipient country, and measures for the protection of personal information taken by the recipient third party, shall be provided to the individual, except in the following cases:

- where the recipient country is a country that is recognised by the Personal Information Protection Commission as having a personal information protection system that is on level with that of Japan (ie, currently the EU and the UK); and
- where the recipient third party has developed a system necessary for continuously taking measures equivalent to the measures to be taken by a business operator handling personal information in Japan (equivalent measures).

In the case of the first point, measures necessary to ensure the continuous implementation of equivalent measures by the recipient are required, and in the event of a request by the individual, the provider shall be obliged to provide them with information on such measures. Therefore, it is preferable to prepare the information to be provided in advance.

Response to the revised Act on the Protection of Personal Information

Healthcare data, especially information obtained in clinical trials, is often registered in overseas databases such as ClinicalTrials.gov, and since it is highly likely that overseas third parties will obtain such information, providers handling healthcare data will need to respond to the above-mentioned revisions to the Act on the Protection of Personal Information. In addition to clinical trial data, when personal data is stored on overseas servers, it is possible that such acts may be deemed as the provision of personal data overseas; therefore, such providers will also need to respond to the aforementioned revisions.

Remote Clinical Trials

Recently, in Japan, "remote clinical trials" have begun to increase. A remote clinical trial is clinical research for approval of a drug or medical device, in which a patient participates remotely, such as from home. Although the introduction of remote clinical trials had not progressed due to concerns about cost-effectiveness, the spread of COVID-19 increased the tendency for people to stay at home and, thereby, increased the necessity for remote trials.

Participants can use smartphone apps to partially conduct clinical trials at nearby medical institutions or at home, saving travel time. Pharmaceutical companies can also expect a reduction in the costs and time of clinical trials, making the development of new drugs more efficient.

In the spring of 2020, the MHLW released guidelines on how to proceed with clinical trials during the COVID-19 pandemic and, by presenting a certain concept of remote clinical trials, made it easier for pharmaceutical companies to introduce remote clinical trials. However, while clinical trials are required to be explained and agreed to in writing, in accordance with the Good Clinical Practice standards, no clear rules for remote clinical trials have currently been established. In the near future, the MHLW intends to compile

guidelines on the elements to be considered when conducting remote clinical trials.

Medical AI

In recent years, the use of artificial intelligence (AI) has gradually resulted in more efficient work, collection and utilisation of medical data, reduction of the burden on patients and provision of information in the healthcare setting in Japan. Previously, AI-organised diagnostic interview information and AI-analysed medical images have been the main components of medical AI. Although approximately 20 medical devices have been officially approved by the MHLW, most of them are medical devices that analyse images by AI.

According to the notification from the MHLW in 2018, when providing treatment using AI medical devices, it is necessary for a physician to be the primary provider of diagnostic treatment and for a physician to be responsible for making the final decision. Therefore, at present, AI is only a tool for presenting information on the medical process and is not permitted to make definitive diagnoses for patients. In the future, the development of AI that can reproduce physician examinations, such as visual examinations, auscultation and palpation, is anticipated.

Metaverse

Companies from a variety of industries have recently explored the possibility of utilising metaverse applications in the healthcare field. For instance, Juntendo University and IBM Japan, Ltd commenced collaborative research with the goal of establishing medical services using the metaverse and are now verifying its effectiveness in clinical sites, which is expected to lead to providing better medical care for patients and their families. As part of the joint research, Juntendo Virtual Hospital, which resembles the real-life Juntendo University Hospital, has been established wherein patients can walk around and read explanations about the virtual hospital. In addition, Astellas Pharma Inc is developing a metaverse service to hold online symposiums which allows for two-way communication between medical personnel, creates a sense of presence and allows for random communication that could not be realised through existing web-based symposiums.

MEXICO

Law and Practice

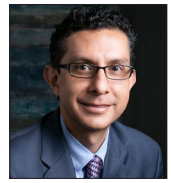
Contributed by:
Bernardo Martínez-Negrete Espinosa, Lisandro Herrera Aguilar and Luis Francisco Marin Tijerina
Galicia Abogados, SC

Contents

Galicia Abogados, SC has a life sciences practice which offers assistance and advice on the regulatory aspects of the manufacture, importation, exportation, release, sale, labelling, promotion, advertising and distribution of pharmaceutical products, medical devices, human vaccines, cannabis derivatives, vaping devices, food and beverages, food supplements, health supplies, cosmetics and pharmaceutical facilities, including clinical data protection and intellectual property of medicines and medical devices. With a team comprised of a partner, a counsellor, four associates and two law clerks based in Mexico City, the firm's life sciences practice represents leading pharmaceutical companies, medical device manufacturers, hospitals, food and food supplement companies, clinical trial sponsors, think tanks and trade associations in life sciences-related matters in Mexico. Its advice in the life sciences sector is mainly focused on public-private partnerships; mergers, divestitures, acquisitions, manufacturing, licence, and joint ventures; the development of different sorts of devices and applications regarding digital health; regulatory, sanitary, and environmental aspects of the planning, construction and operation of hospitals; and human clinical trials.

Authors

Bernardo Martínez-Negrete Espinosa is a partner at Galicia Abogados, with extensive experience in commercial and regulatory aspects of the life sciences industry, and experienced in infrastructure, project finance and mergers and acquisitions. He mostly advises pharmaceutical companies in M&A transactions and on regulatory aspects related to marketing authorisations, divesture of assets, vaccination projects, public procurement, manufacture, supply and distribution of medicines, human clinical trials, construction and operation of pharmaceutical facilities and commercialisation of medicines.



Lisandro Herrera Aguilar is a counsel at Galicia Abogados, with a highly specialised understanding of the healthcare and pharmaceutical sectors, and is a recognised expert in health regulation, governmental procurement processes, pharmaceutical regulation, compliance, small and large molecules medicines, medical devices and digital health. Currently, he acts as counsel in the New Technologies Promoting Council of the Mexican Health Foundation (Funsalud).

Contributed by: Bernardo Martínez-Negrete Espinosa, Lisandro Herrera Aguilar and Luis Francisco Marin Tijerina, **Galicia Abogados, SC**

Luis Francisco Marin Tijerina is a senior associate at Galicia Abogados and advises clients on regulatory matters related to pharmaceutical products, innovative and generic drugs, high-technology equipment, biotechnology, food supplements and medical devices, as well as clinical studies, cosmetics and personal hygiene products, food, alcoholic and non-alcoholic beverages, digital health, tobacco products, toxic and controlled substances, among others. He is also focused on advising clients on consumer protection matters, security and product liability in many sectors of the consumer industry.

Galicia Abogados, SC

Blvd. Manuel Ávila Camacho, 24
7th floor
Lomas de Chapultepec
Mexico City 11000
Mexico

Tel: +52 55 5540 9200
Email: contacto@galicia.com.mx
Web: www.galicia.com.mx/en/

Contributed by: Bernardo Martínez-Negrete Espinosa, Lisandro Herrera Aguilar and Luis Francisco Marin Tijerina, Galicia Abogados, SC

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

From a general perspective, digital solutions for health and health-related matters are a reality and are frequently used. The benefits of digital solutions for patients, healthcare professionals and authorities are evident, but still, there is room for improving regulation. In Mexico, there are no specific regulations in place for these digital solutions, other than general regulations applicable to certain aspects of such technologies (such as data protection, sanitary regulation, IP and cybersecurity, among others).

From a healthcare provider's perspective, using digital solutions represents the opportunity to improve the quality of medical care and optimise patient management. These technologies enable providers to access real-time clinical information, perform remote consultations, make more accurate diagnoses and provide personalised treatments. Implementing these digital solutions will increase providers' operational efficiency, reduce costs and improve communication between different healthcare professionals.

From a patient's perspective, the use of digital solutions allows the patient to access their medical information anytime and anywhere, to receive remote medical assistance and digital drug prescriptions, among other benefits. On the other hand, the use of mobile apps, wearable devices and online platforms helps patients to monitor (in real time) their health condition.

From a regulatory perspective, the sanitary authority oversees regulating and supervising healthcare products and services in Mexico. As these technologies evolve, regulators must ensure that regulation promotes safety, quality, confidentiality and efficacy of health data collected through digital technologies.

Technology platforms that collect and store data play an essential role in generating clinical evidence and improving patient care; unfortunately, there is no regulation for these platforms despite the privacy regulation applicable to personal data. These technologies enable efficient data collection and subsequent analysis in the context of medical interventions, such as surgeries. The interaction between technology platforms and clinical evidence contributes to more informed, evidence-based care, resulting in improvements in health.

1.2 Regulatory Definition

According to the National Centre for Health Technology Excellence (CENETEC), which is as a deconcentrated organism of the Ministry of Health, digital health, which is a broader concept, is defined as the rendering of health services using information and communication technologies, when physical interaction is not necessary, with the purpose of continuing patient care, in this case, is not only related to medical services but rather to health-related services. Digital medicine is the rendering of health services, where healthcare professionals and patients are located in different places, using information and communication technologies to exchange information for the diagnosis, treatment and prevention of diseases and injuries, as well as for medical continuing education.

Besides these definitions and some guidelines issued by Cenetec (which are not compulsory), there are few references in the General Health Law and its regulations with respect to digital health, digital medicine, electronic prescriptions, digital medical files and information and communication technologies. That being said, there

is no list of matters covered by digital health or digital medicine; the analysis is done based on the general regulation applicable to health services and medical devices.

1.3 New Technologies

The development of digital health technology (both digital healthcare and digital medicine) in Mexico is now driven by various stakeholders including start-ups (predominantly comprised of technology firms), healthcare providers (such as hospitals and academic institutions), as well as investors.

Key technologies in digital healthcare are based on mobile applications (apps), wearables and other devices. The development of technologies for digitalising healthcare in Mexico has been gaining momentum as a result of the COVID-19 pandemic, where digital healthcare has been used for optimising health of patients, by being able to monitor certain health indicators and anticipate potential health issues. On the other hand, digital medicine has been driven by telemedicine, artificial intelligence (mainly in the diagnosis field), electronic health records and digital prescriptions, and other developments that improve medical care from a healthcare professional standpoint.

1.4 Emerging Legal Issues

The most relevant legal issue in digital health is the lack of regulations. As at the time of writing in 2023, specific legislation governing digital health or digital medicine in Mexico is scarce and dispersed in different pieces of legislation.

Additionally, there is a gap between regulation and practice. For instance, digital prescription is allowed by the Health Input Regulations; however, its implementation has faced some barriers, since the regulation applicable to the supply of medicines by pharmacies obligates patients to provide the pharmacies with a physical prescription (complying with certain elements, including the signature of the doctor). Therefore, it is necessary to update the whole legal framework for digital prescriptions to become a reality (for example, allowing the use of electronic signature in such prescriptions).

1.5 Impact of COVID-19

COVID-19 accelerated enormously the use of digital health and digital medicine; such technologies allowed healthcare professionals to remain connected with their patients and provide essential treatments and diagnoses in challenging situations (without compromising the health of such physicians).

There are several examples of digital health initiatives across the country, that were implemented to face the COVID-19 pandemic, such as:

- a high-performance broadband satellite network that connects hospitals and healthcare institutions for better information integration processing;
- an electronic platform exclusively designed for hearing-impaired individuals providing crucial COVID-19 diagnostic support serving Mexicans across Puebla; and
- some states developed mobile applications to facilitate self-diagnosis of COVID-19.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

The Federal Commission for the Protection Against Sanitary Risks (*Cofepris* being its Spanish acronym) is the regulatory and enforcement agency for the digital health industry. This author-

ity is responsible for verifying the quality, efficacy and efficiency of health inputs, including services, medicines and medical devices.*Cofepris* is in charge of granting the marketing authorisations for software as a medical device.

Additionally, the Federal Consumer Protection Bureau is the government agency responsible for safeguarding and promoting consumer rights; this agency is focused on commercial and promotional matters.

Regarding the self-assessments and reporting obligations from healthcare institutions, as digital technologies used in health matters are not regulated directly under the Mexican legal framework, there is no legal requirement to self-assess or report any specific matter related to digital medicine or digital health.

2.2 Recent Regulatory Developments

There have been few developments regarding digital healthcare activities. Many of those efforts have been addressed in separate regulations (rather than a single set of rules governing digital health). For example, in December 2021, a new regulation regarding software as a medical device was issued. In May 2023, a new General Law on Humanities, Sciences, Technologies and Innovation was enacted; such law will affect research and development for technologies in the healthcare sector but not necessarily in a positive way, since such new law (among other topics) (i) allows the government to have centralised control over the areas of research and innovation in which public funds are going to be allocated and (ii) provides that research and development activities and projects (with public funds) have to be based on a Special Programme to be developed by the Federal Government (which can be biased). Other drafts of initiatives are being discussed in Congress but, so far, Mexico lacks state-of-the-art legislation that specifically governs the development and use of digital health and digital medicine.

There are a few other draft regulations underway regarding digital health. Some of these include artificial intelligence, cybersecurity, digital health as an ecosystem, electronic clinical records and digital prescriptions; however, these are still pending to be approved by the Mexican Congress.

There is a particular bill, submitted by congressman Éctor Jaime Ramirez Barba on March 2021, the main purpose of which is to develop a legal framework that allows the use of digital technologies in health in an ethical, safe, reliable, equitable and sustainable manner. Other bills are focused on electronic clinical records and digital prescriptions.

2.3 Regulatory Enforcement

Cofepris is the enforcement agency regarding health matters.

The administrative process shall be initiated by a verification visit to an establishment, whereafter an official action will be issued containing the results of such verification and informing about the irregularities identified. The establishment involved should answer with the corrective actions or its arguments overcoming the findings. A resolution will be issued in which sanctions may be imposed. This resolution can be challenged before a federal court. *Cofepris* has the authority to impose sanitary measures during the administrative process, at any time.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

The Federal Consumer Protection Bureau (PROFECO) regarding commercial matters and the National Institute for Transparency, Access to Information and Protection of Personal Data (INAI) for data protection matters, are the non-healthcare regulatory agencies that could be involved in digital healthcare.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

Preventive care includes those medical activities which are generally advertised through campaigns to prevent a specific disease or condition. Conversely, there is no definition for "diagnostic care"; however, it can be defined as those medical activities related to the finding of a specific pathology in a patient.

Preventive care is focused on awareness campaigns about the consequences of specific diseases or conditions, by creating consciousness among the population; these actions are mainly managed by the Ministry of Health at a national level. The diagnostic actions are done by each healthcare professional following the medical guidelines or the Mexican Standard Norms.

4.2 Increased Preventative Healthcare

There are some campaigns and legal actions that have been conducted by the Mexican government to be considered as preventive care:

- inclusion of the COVID-19 vaccine in the Universal Vaccination Programme;
- the prohibition of edible oils and fats in food and non-alcoholic beverages known as trans fats;
- the implantation by the IMSS (National Health Service for private sector employees) of an app called heart attack code (*Código Infarto*. The purpose of this app is for an infarcted person with chest pain symptoms, shortness of breath or fainting, to receive medical care within 30 minutes or less. The app is beneficial for around 55 million users through 344 medical units equipped to provide this service, including 11 High Specialty Medical Units, 181 Regional or Area General Hospitals, and 152 Family Medicine Units; and
- the incorporation of preventive seals in food with added sugars, carbohydrates, oils and fats, calories and sodium.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

In Mexico, wellness and fitness data is regulated under data protection laws and it is considered as health-related data, which is indeed more sensitive than any other kind of personal data. Any personal data that, if it is exploited, might lead to discrimination, or pose severe harm to the data owner, is sensitive personal data. The main rule is that the owner of the personal data must provide their written consent before any processing of that data may take place.

On the other hand, from a sanitary standpoint, developers of apps and wearables that manage wellness and fitness data, shall carefully review the way in which such data is provided to the user of the app or the device, in order not to be considered as providing medical advice (which

would require a licence to render professional medical services).

4.4 Regulatory Developments

Preventive care is a goal of the national health system and the Ministry of Health is responsible for that. Preventive care has been focused on specific diseases such as cancer, diabetes, hyper cholesterol, AIDS and others; for these, the Ministry of Health has created Mexican Official Standards and clinical guidelines to prevent these diseases. Moreover, vaccination and immunisation policies have also been created; nevertheless, due to the COVID-19 pandemic, vaccination rates have decreased considerably.

4.5 Challenges Created by the Role of Non-healthcare Companies

There two main challenge of non-healthcare companies entering the market, which are:

- compliance with the provisions set forth under data protection law; the National Institute for Transparency, Access to Information and Protection of Personal Data (INAI) (which is the authority in charge of granting access to public information and protecting personal data) has been conducting extensive reviews (and in many occasions imposing penalties) of the parties responsible for the processing of sensitive personal health data; and
- compliance with the health regulation regarding the promotion of products and services.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

Several technological solutions have been introduced throughout Mexico's hospitals to enhance patient care and make better use of connected medical equipment, for example:

- electronic medical records – doctors have been able to access and keep updated the clinical information of their patients. This allows various departments and healthcare professionals to easily communicate with one another and seamlessly share data, which ultimately leads to improved healthcare coordination and quality; and
- connected medical devices – vital sign monitors and other telemedicine devices have enabled remote monitoring of patients. These gadgets provide data to doctors in real-time, which makes it easier for doctors to spot potential health issues early on.

Remote health in Mexico has been significantly supported by technological advancements, such as:

- telemedicine – virtual medical consultations are now possible because of widespread videoconferencing platforms and software designed for mobile devices. Patients can communicate with their healthcare providers via the use of videoconferencing, which helps them save time and money, and provides quicker access to medical treatment; and
- patient monitoring – gadgets that can keep track of patients suffering from chronic conditions have made this possible. Patients diagnosed with diabetes, for instance, can use

gadgets that detect their glucose levels and remotely exchange the data with their treating doctors. This makes it possible to continuously evaluate their health situation and make appropriate modifications to their therapy at the appropriate moment.

A substantial amount of progress has been made in home care in Mexico after hospital release because of technological developments. Some advancements worth noting are:

- post-operative telemonitoring, which allows patients who have just had surgery to be remotely monitored at home using linked electronic equipment. Medical professionals can track a patient's progress toward recovery, identify any issues that may arise, and provide advice even if the patient is not at the hospital; and
- digital medicine and mobile applications – patients now can obtain individualised medical advice, access their own health information, and receive prescription reminders all from their mobile devices thanks to the development of mobile apps. These applications facilitate home health care and encourage people to take an active role in their own medical treatment.

5.2 Legal Implications

It is possible to incur civil liability because of adverse healthcare outcomes; this responsibility could be of the healthcare professional, the hospital and/or the manufacturer of the health input. All these responsibilities are based on the damages caused to the victim, who may seek compensation from the party responsible for such damage.

Moreover, healthcare professionals, hospitals and developers can be liable for infringement of the General Health Law and its regulations; in this case, all of them could face administrative sanctions (such as fines), the healthcare professional could be disbarred and the developer could face the cancellation of its marketing authorisation, among other things, such as product seizures, service bans and facility closures.

5.3 Cybersecurity and Data Protection

The main risk identified for the cloud computing environment is that security may be violated through cyber-attacks, which could lead to data loss or breaches in confidentiality, resulting in the infringement of data protection laws.

On the other hand, the key risks assessed for on-premises and local computing environment are non-authorised access (this could lead to data leaking or even identity theft), and service interruption (that can be a result of a cyber-attack that intends to slow or even shut down this services).

Most cybersecurity risks may be addressed in the contracts or agreements between third parties and healthcare institutions, in which the liability for each of the parties is clearly outlined and specific performance standards (including emergency response, remedial actions, access to audits, among others) are agreed upon. In terms of data protection laws, the party in charge of collecting the personal data will be the one responsible before the authority. Thereafter, indemnifications may be adopted in the contract in case of any economic sanctions.

5.4 Proposed Regulatory Developments

None of the initiatives reviewed by the authors regarding digital health matters have addressed regulations for specific internet of things (IoT). Nowadays, congressmen are focusing on general provisions that may allow the regulation of

digital health and digital medicine without entering into a further analysis (such as internet of medical things).

However, according to Mexican Official Standard NOM-241-SSA1-2021, Good Manufacturing Practices for medical devices (which became effective on 21 June 2023), software may be classified as a medical device if it is used for one or more medical purposes, operates on general computer platforms and is used by itself or together with other products.

As mentioned above, although there is no clear legislation in Mexico on the IoT, regulators are (slowly) starting to craft regulations regarding digital technology focused on health matters, that may eventually evolve into regulating IoT.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

The Mexican Official Standard NOM-241-SSA1-2021, Good Manufacturing Practices for medical devices, which became effective on 21 June 2023, is the first legal provision in Mexico to regulate software as a medical device. As a result, software is considered a medical device if it meets the following criteria: (i) it is used for one or more medical purposes; (ii) it can run on general computing platforms; and (iii) it can be used alone or together with other products (such as a module or other medical devices). Please note, however, that software that runs only on a specific physical medical device is exempt from this classification and will not require registration to be marketed within Mexican territory.

AI and machine learning do not have a specific regulation in Mexico; however, as both of them could fill in the definition of software as a medical device, they could be considered as such if the above-mentioned criteria are met.

Whether software meets the above-mentioned criteria is relevant from different perspectives. For example, considering that a medical device can only be sold in specific establishments (ie, pharmacies), promotion of the product has to be done, exclusively, to healthcare professionals, technovigilance reports have to be submitted once a year to *Cofepris* and the marketing authorisation is subject to renewal.

The authority with jurisdiction over software as a medical device is *Cofepris* and it is in charge of validating the quality, safety and efficacy of the software. Among its powers, it can impose sanitary measures such as the prohibition of selling the software, and fines to the distributor and manufacturer. Additionally, the owner of the marketing authorisation must be aware and comply with the Data Privacy Law, which established an obligation to present a data privacy notice to communicate the uses of the data collected by the software. Moreover, health data is considered sensitive personal data and therefore if this data is to be transmitted to a third party, then it has to be accepted by the owner of the data.

Companies outside the care industry must comply with specific requirements such as an operation notice and designate a sanitary responsible if they are willing to register their software as a medical device; conversely, companies that keep their software outside of the definition of medical device have to be careful of the intended uses and claims of the product to avoid any sanctions from *Cofepris*.

7. Telehealth

7.1 Role of Telehealth in Healthcare

Mexico has seen rapid expansion in the use of telehealth. Telemedicine has made possible the creation of "virtual hospitals," which are places where patients may get medical treatment online by using numerous forms of communication technology and information systems. These virtual hospitals have made it possible for patients located in remote regions to get specialist medical treatment by providing access to medical professionals.

The advent of telehealth has made it feasible to provide medical care to patients who are located at a distance from the provider. This has proven to be particularly helpful in circumstances that make it difficult or expensive to physically go to the patient. Telehealth allows medical experts to make diagnosis, monitor patients, provide medical advice and issue prescriptions without the need for patients to physically attend the clinic.

Patients now can get first medical treatment in a more expeditious manner thanks to the advent of telehealth, which has made it possible to utilise virtual consultations as a gateway to medical care. Patients may conduct medical consultations with healthcare experts remotely, without having to travel to a clinic, by using communication software or videoconferencing technology. This has shown to be particularly helpful in situations involving regular consultations, the follow-up of patients with chronic diseases and early medical assistance.

Regarding cross-border telehealth, it is worth considering the requirements of having a professional licence to practice medicine in different jurisdictions. Patients from various states, provinces, or even countries can receive medical assistance through telehealth. However, compliance with the specific regulations and legal requirements of each jurisdiction is required. This includes procuring the essential licences and authorisations to practice medicine in the location where the patient resides, as well as complying with privacy and data protection laws in each jurisdiction.

7.2 Regulatory Environment

During the COVID-19 pandemic, the Federal government declared a state of emergency, which implied that the government was allowed to purchase any health input or any other material that could help in the pandemic without the need to follow the procurement process; several emergency authorisations for vaccines and medicines were granted. Furthermore, the import of health inputs without marketing authorisations was allowed in order to face the COVID-19 emergency.

Online platforms are regulated in a general manner; there are no specific provisions used as part of digital medicine or digital health.

7.3 Payment and Reimbursement

Reimbursement in Mexico is not like in Europe or other countries. In Mexico, with respect to patients affiliated to social security, health services, including medicines and some medical devices, are prepaid through social security contributions done by workers and employers on a monthly basis (such mechanism is similar to an insurance scheme, but managed by the government either through IMSS or ISSSTE (National Health System for governmental employees)). For patients without social security, the health services, including medicines and medical devices, are free but limited to those treatments and medicines defined by the government (such

services are funded by the government and the states through public budgetary resources).

Despite the above, public health institutions have several digital health and digital medicines programmes for their patients.

In the private sector, the reimbursement from the insurance company will depend on the terms and conditions of the applicable patient's insurance policy. Therefore, there is no general rule.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

The main regulatory issue regarding the internet of medical things is that, at this time, there are no specific provisions that apply to goods or services that are digitally delivered in the health sector (including digital assistants and the internet of medical things). However, indirect regulation applies in general terms to the digital technologies applied to health-related matters.

If a product (ie, hospital beds, wearables, implantable, etc) will help in medical care for the purpose of diagnosing, preventing, treating, rehabilitating or following up on pathologies, as well as for caring for and promoting health, it will be considered a health input and applicable provisions shall be met in this regard (eg, having an operation notice, securing a marketing authorisation and importation permits, among others).

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

In general terms, 5G networks can provide additional benefits to telehealth, IoT and medical treatments, such as faster data transfer rates both up/downstream and less latency, providing a more responsive user experience. Greater connectivity allowing multiple devices to be linked simultaneously while increasing device support capacity ensures less congestion across the network, resulting in far higher reliability/stability of the connection itself.

However, the 5G network implies a relevant investment in infrastructure (mainly hardware) to obtain the benefits of the network. Additionally, the gap between urban and rural areas could increase considerably. Mexican health system infrastructure is obsolete; therefore, it is likely that the medical devices that are currently in use may not support the 5G network. Moreover, for digital medicine, it is necessary that both patients and healthcare providers use the same network, otherwise the speed of transmission will be driven by the lower of the two.

Contracts between health institutions and 5G providers should clearly define expected parameters around performance, availability, quality of service covering all backup solutions, redundancy and robust measures regarding security; mainly with respect to patient confidentiality.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

According to the Federal Law for the Protection of Personal Data Held by Private Parties, the level of protection afforded to health-related data in Mexico is greater than that given to any other type of personal data; this is because health-related data is considered sensitive personal data, which means that misuse of the information could result in discrimination or constitute a severe threat to the data proprietor. As a general rule, all processing of personal information requires the owner's written consent.

In addition, databases containing sensitive personal data can only be kept when their legitimate and specific purposes are justified by the responsible party, consistent with the latter's activities or purposes, and reasonable efforts must be made to limit the processing period to the bare minimum. However, anonymised health data is excluded from the scope of data protection laws, as such data cannot lead to the identification of a person.

Depending on the nature of the data, the intentionality of the action or omission constituting the violation and the financial standing of the data controller, a violation of data protection laws can result in significant fines. In addition, violations of regulations pertaining to sensitive personal data (for instance, health data) may result in sanctions and penalties. When attributable to the data controller, breaching the security of databases, premises, computer programs and equipment is considered a criminal offence punishable by up to three or five years in prison, or twice as long if the breach involves unlawful treatment of sensitive personal data.

From the regulatory point of view, the collection and use of health data are highly regulated, for instance, patients must grant their consent to collect their health data, and informed consent must express the use of the data. Informed consent must comply with specific requirements that are laid down in the regulation of clinical trials. Moreover, the information on the health records belongs to the patient, and its access is restricted to their healthcare provider.

Wearables and other devices, that collect personal health information, that are not considered medical devices, do not have to comply with the health regulation for data collection, since the goal of collecting that information is out of the scope of the health law. Nevertheless, they have to comply with data privacy regulations and therefore a privacy notice must be in place for users to accept the collection and use of their data.

It is strongly suggested that any processing of raw health data be preceded by a privacy notice in Spanish that complies with data protection laws and describes the purpose of the processing in detail; this can be reviewed by the National Institute for Transparency, Access to Information and Protection of Personal Data (INAI). As the Health Authority has powers to review the collection of health data, it is important to obtain informed consent for the collection of health data for medical purposes.

Please note, however, that as anonymised data cannot identify a subject, it does not fall within the range of data protection laws. Hence, its use, disclosure and all other relevant activities related thereto comprise a business decision.

Despite the overlap of these regulations, they are aligned in the sense that personal health data

is relevant for the patient/owner, and therefore higher restrictions shall be in place to guarantee the proper treatment of the data. Nevertheless, it is important to comply with both regulations.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

AI used within the healthcare sector should always be augmented intelligence, since human knowledge and decisions shall always prevail. However, AI is a very effective tool for healthcare professionals to obtain information related to diseases and their treatments or event to manage clinical records (as long as the personal information is shared in compliance with applicable legal provisions).

One of the most relevant risks of electronic medical records is that they may be subject to misuse of personal sensitive data or cybersecurity attacks.

In Mexico, regulation has still not defined the optimal standard for securing businesses against cyber threats. As part of an overarching legal framework for safeguarding individual data protection concerns, those serving as controllers or processors must develop a reasonable network defence and shall routinely perform vulnerability assessments regarding technical infrastructure.

11.2 AI and Machine Learning Data Under Privacy Regulations

Currently, some initiatives are being discussed in the Mexican congress regarding AI (such as the draft of Law for the Ethical Regulation of Artificial Intelligence and Robotics (*Ley para la Regulación Ética de la Inteligencia Artificial y la Robótica)* that was introduced for discussion in Congress in May 2023). However, as it is a complex (and rather unexplored) topic, Mexican representatives tend to be extremely cautious and risk averse when discussing and analysing such projects, which has caused the country to lack an appropriate regulation around AI.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

As digital healthcare technologies are still not regulated under the Mexican legal framework, healthcare companies using digital health technologies are facing the same issues as non-healthcare companies (which mainly relate to compliance with the provisions provided in the data protection laws and in the consumer protection law).

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

For telemedicine to be suitable to be implemented within a healthcare institution, it is required that a platform allows doctors and patients to communicate with one another in real time through digital channels. To do this, secure systems for videoconferencing, data transfer and the maintenance of electronic medical records need to be developed. In addition, to have equal access to telemedicine services throughout Mexican territory, there must be a consistent connection across the country at a high speed. This is particularly important in more rural regions.

To harness the potential of machine learning in the healthcare industry, information technology systems that can gather, store, and evaluate

enormous amounts of clinical data are required. This implies having cloud storage infrastructures and scalable database systems, in addition to the development of machine learning algorithms that are appropriate for the analysis of clinical data. Besides, stringent security and privacy precautions have got to be taken for complying with applicable provisions of data protection laws.

For integrating IoT, an IT infrastructure is required that can enable the connection and interchange of data between medical and computer systems, operated by networks that are both trustworthy and safe. Interoperability standards shall be developed, making it possible for devices to be seamlessly integrated into healthcare settings. In addition, security and privacy standards need to be devised to safeguard the information that is produced and ensuring compliance with data protection laws.

Together with the IT infrastructure referred to before, increasing the reach of broadband internet and embracing new technologies like fibre optics will allow safer and dependable data transmissions, with additional security measures, such as data encryption and authentication, which should be in place.

13.2 Data Management and Regulatory Impact

There have not been any proposed regulations in addition to those that are already in force; therefore, in terms of data protection laws, data controllers are responsible for conforming to legal principles and obligations, such as implementing appropriate security measures to protect data from loss, theft and unauthorised use or access.

14. Intellectual Property

14.1 Scope of Protection

In Mexico it is possible to obtain patent protection for an invention, regardless of the field of technology, if it complies with the following:

- being novel – ie, not being in the state of the art;
- being the consequence of inventive activity – ie, not being apparent or noticeable; and
- the subject of industrial application – ie, the possibility that the invention could be used in any industry.

Databases, algorithms, software, and any technology reflected in writing are not subject to be patentable in Mexico. Nevertheless, the Federal Copyright Law provides protection for databases, algorithms, software and any technology reflected in writing, which basically states that copyright protection begins once the work is fixed on a material support (regardless of its merit, purpose or mode of expression). Nonetheless, for exercising a copyright action before a third party, it must be registered before the National Institute of Copyright.

A trade secret is the information of an industrial or commercial application that the person exercising legal control keeps confidential, which means obtaining or maintaining a competitive or economic advantage over third parties in the performance of economic activities and for which adopted means or systems to preserve its confidentiality and restricted access exist.

The type of protection, whether it is a patent, copyright or trade secret, will depend on the invention per se and a case-by-case analysis.

Regarding the possibility to protect an invention or copyright that has been created by AI, machine learning, or any other type of software, in Mexico it is not possible to do so because the Federal Law for the Protection of Intellectual Property and the Federal Copyright Law establishes that the inventor or the creator must be a human being.

14.2 Advantages and Disadvantages of Protections

As referred to above, algorithms, databases, software (except those classified as medical devices) and any written technology will be considered a work and will be subject to copyright protection. These works are not required to be registered before the National Institute of Copyright as the protection commences when the work is fixed on a material support (regardless of its merit, purpose or mode of expression).

Yet, to exercise copyright rights before a third party, registration before the copyright authority is recommended, as this will mean that the right is duly recognised.

14.3 Licensing Structures

Licensing intellectual property rights always requires extra caution and a written agreement plays an essential role to establish the scope and time of the licence, exclusivity if any, territorial delimitation, the obligations and rights of each party, royalties or compensation that the licensee shall pay to the licensor and whether the licence will be registered.

A relevant clause in all licensing agreements is the prosecution of potential infringements, including the dispositions regarding which party will be responsible for making the decision to initiate the action, and what would happen if the party responsible for making that decision refuses to act and there are material or economic damages to the other party.

Furthermore, it is relevant to include a transitional period at the beginning and the end of the agreement to continue the commercialisation of the product. Additionally, it is important to establish which party will be responsible for obtaining the marketing authorisations from the authorities, if any, and what will happen with those marketing authorisations at the end of the licence agreement – ie, if they are going to be assigned or not, who will pay for the assignment and the obligation to collaborate in the assignment of rights.

14.4 Research in Academic Institutions

Authorship of inventors and authors must be recognised as such in the patent or copyrights registration, regardless of the agreement with the university, inventor or healthcare institution.

If the inventor/author is an employee of the university or healthcare institution, then the Federal Labour Law applies, and it states that employees will be the author of inventions made for their employer, but the employer retains ownership of the inventions and the right to exploit the patents or copyrights.

However, if the inventor/author is not an employee, but rather an independent service provider, the terms of the intellectual property rights will be those laid down in the service agreement, but the authorship of the invention/copyright must be for a physical person.

According to the New General Law on Humanities, Sciences, Technologies and Innovation (*Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación)* enacted in May 2023, copyright and industrial property rights over

works and inventions derived from processes of humanistic and scientific research, technological development and innovation financed with public resources, shall benefit and be reserved for the welfare of the people from Mexico. The foregoing is in the terms of the applicable legislation and intellectual property of which the Mexican State is a part.

14.5 Contracts and Collaborative Developments

Any contractual arrangement superseding statutory rules will be considered null, therefore, it shall be aligned to provisions set forth under the applicable legal framework. Bear in mind that the recognition of authorship is compulsory in Mexico, but the exploitation and/or economic rights can be subject to contractual arrangements.

15. Liability

15.1 Patient Care

There have not been cases in Mexican Courts regarding decisions based on digital health technologies, however, based on the liability theories, healthcare professionals and software developers could be responsible for the following.

Civil liability – healthcare professional – based on the fact that the healthcare professional is responsible for the decisions made regarding their patient, they could be liable regardless of whether the decision was made using AI, machine learning or software as a medical device; this will be an extra-contractual (tort) liability – ie, malpractice case.

Nevertheless, if the decision is based on using software as a medical device, the developer of the software could be liable if the malfunctioning of the software is proven; this will be a product liability.

Moreover, healthcare professionals and software developers can be liable for infringement of the General Health Law and its regulations; in this case, both could face administrative sanctions, such as fines, the healthcare professional can be disbarred and the software developer can face the cancellation of its marketing authorisation, among other things, such as product seizures, service bans and facility closures.

15.2 Commercial

Third-party vendors' products or services can be legally responsible by extra-contractual liability (tort) or by contractual responsibility.

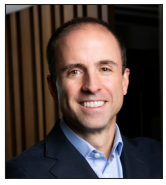
In the case of tort responsibility, it is necessary to prove that the third party was negligent in the care of the product or rendering of the services and to establish a link between the fault and the damage caused by that conduct. If the responsibility arises from contractual breach, it will depend on the terms of the contract entered with the third party, in which the liability distribution should be detailed.

Trends and Developments

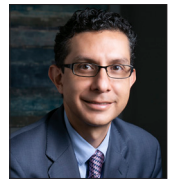
Contributed by:
Bernardo Martínez-Negrete Espinosa, Lisandro Herrera Aguilar and Luis Francisco Marin Tijerina
Galicia Abogados, SC

Galicia Abogados, SC has a life sciences practice which offers assistance and advice on the regulatory aspects of the manufacture, importation, exportation, release, sale, labelling, promotion, advertising and distribution of pharmaceutical products, medical devices, human vaccines, cannabis derivatives, vaping devices, food and beverages, food supplements, health supplies, cosmetics and pharmaceutical facilities, including clinical data protection and intellectual property of medicines and medical devices. With a team comprised of a partner, a counsellor, four associates and two law clerks based in Mexico City, the firm's life sciences practice represents leading pharmaceutical companies, medical device manufacturers, hospitals, food and food supplement companies, clinical trial sponsors, think tanks and trade associations in life sciences-related matters in Mexico. Its advice in the life sciences sector is mainly focused on public-private partnerships; mergers, divestitures, acquisitions, manufacturing, licence, and joint ventures; the development of different sorts of devices and applications regarding digital health; regulatory, sanitary, and environmental aspects of the planning, construction and operation of hospitals; and human clinical trials.

Authors



Bernardo Martínez-Negrete Espinosa is a partner at Galicia Abogados, with extensive experience in commercial and regulatory aspects of the life sciences industry, and experienced in infrastructure, project finance and mergers and acquisitions. He mostly advises pharmaceutical companies in M&A transactions and on regulatory aspects related to marketing authorisations, divesture of assets, vaccination projects, public procurement, manufacture, supply and distribution of medicines, human clinical trials, construction and operation of pharmaceutical facilities and commercialisation of medicines.



Lisandro Herrera Aguilar is a counsel at Galicia Abogados, with a highly specialised understanding of the healthcare and pharmaceutical sectors, and is a recognised expert in health regulation, governmental procurement processes, pharmaceutical regulation, compliance, small and large molecules medicines, medical devices and digital health. Currently, he acts as counsel in the New Technologies Promoting Council of the Mexican Health Foundation (Funsalud).

Contributed by: Bernardo Martínez-Negrete Espinosa, Lisandro Herrera Aguilar and Luis Francisco Marin Tijerina, **Galicia Abogados, SC**

Luis Francisco Marin Tijerina is a senior associate at Galicia and advises clients on regulatory matters related to pharmaceutical products, innovative and generic drugs, high-technology equipment, biotechnology, food supplements and medical devices, as well as clinical studies, cosmetics and personal hygiene products, food, alcoholic and non-alcoholic beverages, digital health, tobacco products, toxic and controlled substances, among others. He is also focused on advising clients on consumer protection matters, security and product liability in many sectors of the consumer industry.

Galicia Abogados, SC

Blvd. Manuel Ávila Camacho, 24
7th floor
Lomas de Chapultepec
Mexico City 11000
Mexico

Tel: +52 55 5540 9200
Email: contacto@galicia.com.mx
Web: Web: www.galicia.com.mx/en/

Contributed by: Bernardo Martínez-Negrete Espinosa, Lisandro Herrera Aguilar and Luis Francisco Marin Tijerina, **Galicia Abogados, SC**

Introduction

According to the World Health Organization, digital health is the use of electronic information and communication technologies in a cost-effective way that supports health and health-related matters, such as medical services, patient monitoring, diagnostics, education and training for healthcare professionals and students, and research and development, among other uses. The concept of digital health is not new; the World Health Organization and other international organisations started using it in the 1990s, but it became widely popular because of the COVID-19 pandemic. As in many other countries, in Mexico, digital health was crucial during the pandemic to continue monitoring patients with chronic diseases that could not attend their health reviews due to the risk of contagion, to create databases of COVID-19 cases, for analysis of COVID-19 symptoms, to monitor people's movement and many other uses.

Now that the pandemic is over, digital health could help the national health system to address its challenges and develop opportunities for improvement of medical services. It is worth mentioning that, lately, the national health system has been under stress because of budgetary cuts, the lack of medicines and healthcare professionals, obsolete infrastructure that has not been renewed, outdated regulation, and amendments to different legal frameworks (from the procurement of medicines to the rendering of medical services to people without social security). On the other hand, the Mexican population is growing and aging, there are high rates of non-transmissible chronic diseases such as diabetes, cancer, and hypertension, which create a lot of pressure on the national health system. Digital health could help to alleviate these problems, but a long-term national policy and state-of-the-art regulation is needed in order to incentivise the use of these technologies.

Regulation

A major problem with technology is that it evolves faster than its regulation, thus creating a gap between what it is regulated and the technology itself. In some countries, governments have issued guidelines and principles to regulate the use of technology in different aspects, including health and health-related matters; in Europe for instance, a special group was created to develop the regulation of artificial intelligence and other technology matters. In Mexico, the National Centre for Technological Excellence in Health (CENETEC) is in charge of developing these types of guidelines and content; however, its opinions and guidelines are not compulsory and are barely known in the sector.

The challenge when drafting regulations applicable to technology is to have not only a long-term perspective, but also to be dynamic, inclusive and open to further review on a regular basis.

In the case of Mexico, the reforms of the legal system regarding digital health have undergone isolated modifications, which seem not to fit the characteristics previously mentioned; therefore there is uncertainty for investors, entrepreneurs, authorities, academia, practitioners, and everybody involved in the digital health ecosystem. The following are some relevant events that have taken place in this sector in the past.

- In 2010, the Ministry of Health appointed the CENETEC to gather information and data regarding the use of information and communication technologies in health to create guidelines and principles that would lead the development of digital health regulation.

Contributed by: Bernardo Martínez-Negrete Espinosa, Lisandro Herrera Aguilar and Luis Francisco Marin Tijerina, **Galicia Abogados, SC**

- In 2012, the obligation of the Ministry of Health (i) to guarantee the interoperability, processing, interpretation and security of the information contained in digital health records and (ii) to allow medical care services to be provided by electronic means in accordance with the regulations issued by the Ministry of Health for that purpose, was established.
- In 2013, as a goal of the national health system, the promotion of health services using information technology was included, and the Ministry of Health was empowered to promote the incorporation, use and exploitation of information and communication technologies in health services.
- Additionally, in 2013, the Telecommunication Reform amended the Federal Constitution, stating that the Executive branch of the government will be in charge of the universal and inclusive digital policy to promote public and private investment in telehealth, telemedicine and electronic clinical records applications.
- In 2018, electronic prescriptions were allowed.
- In parallel over all of these years, CENETEC has published several pieces of soft regulation regarding digital health, telemedicine and other health-related matters; however, its dissemination has not been as wide as it should be.

All of these amendments are isolated efforts, but they are not part of a long-term strategy to address digital health; however, they have been used as a legal stand for those projects that have been implemented in the past years. Unfortunately, the regulation is scarce and lacks precision, leaving several legal topics open and subject to interpretation.

Currently, several bills regarding digital health are being discussed in congress, but none of them have been approved and therefore the gap between reality and regulation is getting bigger every day.

Reality

Today, the use of electronic platforms, webpages, mobile applications, social media, artificial intelligence and other information and communications technologies is a reality and accessible to a large number of people. In Mexico, there are different health services rendered using information and communications technologies, which have provided prompt and timely medical diagnosis and treatment, improved the use of economic resources, and relieved the national health system. The benefits of telemedicine are to thousands of patients with different diseases (such as sclerosis, hypertension, cancer and diabetes, among others), who are vulnerable and need constant medical attention. Some examples of developments in digital health in Mexico are the following.

- Telemedicine has been growing steadily in Mexico, and there are a number of telemedicine providers operating in the country, including private and public hospitals. Telemedicine has proven to be beneficial to provide medical services in rural areas of the country.
- Mobile health apps are a type of software that can be used to track health data, provide health information and connect with healthcare providers.
- Electronic health records are digital systems that store patient health information in public and private hospitals.
- Software as a medical device has been recently regulated in Mexico through an Official Standard Norm and its main characteristic is that it does not require hardware to fulfil the intended medical purpose; it can operate

on general computing platforms, and can be used alone and/or in combination with other products. Software included in a medical device is excluded from this definition.

Moreover, the COVID-19 pandemic accelerated the use of these technologies, and some programmes were launched at federal and state levels, such as:

- a high-performance broadband satellite network to improve communication between the Ministry of Health and hospitals and health centres for the integration, processing and delivery of information;
- a COVID-19 diagnostic programme for hearing-impaired disabled people through the electronic platform of the state of Puebla; and
- the states of Jalisco, Puebla, Nuevo León, Chihuahua and Mexico City, among others, created different mobile applications for the self-diagnosis of their inhabitants, some of which also aim to inform about relevant news related to COVID-19 and provide the location of suspected cases to mitigate contagion within such state.

Similarly, the private sector developed several applications regarding digital prescriptions, telemedicine, medical directories, psychological care and clinical data storage.

Several digital health projects are in place and are helping thousands of patients across the country, but the gap in access to health services and particularly digital health technologies is increasing due to the lack of technological resources (internet access, hardware and software) in rural and remote areas of the country. Furthermore, the regulation applicable to these projects is not clear and has not been properly developed.

Basic Digital Infrastructure

A prerequisite for using information and communication technology is to have a basic digital infrastructure, which means access to internet, software, and hardware to do so (ie, smartphone, tablet or computer). In Mexico, access to the internet and proper hardware is a major concern. For example:

- in accordance with the Inter-American Development Bank, only 19% of households in rural areas have access to internet, while in urban areas, the percentage rises to 62.3% (*El Impacto de la Infraestructura digital en las consecuencias de la COVID-19 y en la mitigación de efectos futuros. Banco Interamericano de Desarrollo. 2020)*;
- of the households that have internet access, the average broadband speed on fixed lines is 42.5 Mbps, while on mobile lines it is 30.8 Mbps, which is below the 50 Mbps that is considered the optimal broadband (*El Impacto de la Infraestructura digital en las consecuencias de la COVID-19 y en la mitigación de efectos futuros. Banco Interamericano de Desarrollo. 2020)*;
- furthermore, according to National Institute for Statistics and Geography (INEGI), in 2019, 44.3% of households in the country had one computer (*Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH): Instituto Nacional de Estadística y Geografía. 2019)*;
- the percentage of the population with access to internet outside their home is 10.7% (*Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH): Instituto Nacional de Estadística y Geografía. 2019*); and
- the population of cell phone users is 75.1%, but not all of them have internet access on their mobile phones (*Encuesta Nacional*

*sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH): Instituto Nacional de Estadística y Geografía. 2019_*.

Challenges

Based on the above analysis, the main challenges in Mexico regarding digital health are as follows.

- Absence or lack of regulation; the regulatory environment for digital health in Mexico is still evolving. This can make it difficult for companies to develop and deploy digital health solutions. As mentioned before, there are several digital initiatives currently discussed in congress, but no clarity as to which of those will become regulation.
- Achieving universal access to digital health services due to the gap between urban and rural areas regarding access to internet, the quality of the broadband, the devices used to access internet, and the availability of computers in households.
- Interoperability; the national health system is fragmented into different health services providers; for instance, the Mexican Social Security Institute (IMSS) is dedicated to workers (with social security) in the private sector, the Social Security Services for State Workers renders services to workers of the public sector at the federal level, the IMSS Bienestar (successor of INSABI and Social Insurance – *Seguro Popular*) is for the people without any social security service and most of the states in Mexico have their own local health public system (ie, according to the Mexican Constitution, the power to render public health services is concurrent among federation and states). In addition to the above-mentioned systems, there are High Specialised Hospitals managed by the Ministry of Health, and some federal governmental entities, such as Pemex, the Ministry of Defence and the Marine Ministry, have their own healthcare services. Finally, there are private healthcare providers. There are patients that use more than one health system (people switch jobs, move from one side of the country to another, or from one neighbourhood to another), so the challenge is to create a single database that can be used at the national level for public and private healthcare providers, regardless of where the patient is and their affiliation to a specific healthcare service provider.
- Information security is an issue that should be of concern. Who will hold the health records of Mexican patients, where will that information be stored, who will have access to it and how it will be used?
- Mexico's healthcare infrastructure is not well equipped to support digital health, not only due to the low broadband internet access but also because of poor hardware and obsolete equipment infrastructure.
- Cultural barriers; people that do not understand technology could be reluctant to use digital health technologies.

Opportunities

There are several opportunities for digital health in Mexico, which include the following.

- Improving access to healthcare – digital health can help to improve access to healthcare by making it easier for people to connect with healthcare providers. This is especially important in rural areas, where there may be limited access to healthcare facilities.
- Reducing costs – digital health can help to reduce costs by making it more efficient to deliver care. For example, electronic health records can help to reduce the amount of paperwork that is required, and telemedicine

can help to reduce the need for in-person visits.
- Improving the quality of care – digital health can help to improve the quality of care by providing more personalised and timely care. For example, mobile health apps can help people to track their health data and share it with their healthcare providers.

Conclusion

Digital health can help improve the national health service and make it more accessible and affordable. However, there are challenges that need to be addressed to unleash the full potential of digital health in Mexico.

The legal system to regulate digital health has to (i) promote open access and interoperability of the different platforms and technologies, (ii) promote research and development of new technologies by providing security of IP rights to developers, (iii) be collaborative, where patients, industry, government agencies, doctors and hospitals are taken into account, (iv) be based on intergovernmental collaboration, best practices and experiences with information and communication technologies, (v) be based on evidence, with a risk approach for patients and users (ie, balancing the potential harm of certain technology with the general benefit that it can create in society) and (vi) be flexible to regulate existing information and communication technologies, and allowing the development and implementation of new ones. This regulation must be focused on long-term benefits and on a national digital health policy.

SOUTH KOREA

Law and Practice

Contributed by:
Kyungsun Kyle Choi, Eui Seok Kim, Myung Soon Chung and Ari Yoon
Kim & Chang

Contents

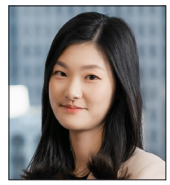
Kim & Chang has a Healthcare practice group that brings unparalleled regulatory, intellectual property, corporate, competition law and litigation expertise to meet the complex needs of clients in the pharmaceutical, animal health, medical device and diagnostics sectors. Formed when Kim & Chang was first established in 1973, the Healthcare practice group has since advised the majority of multinational firms doing business in these sectors in Korea, from established industry leaders to newer digital healthcare companies and start-ups. The firm's highly experienced attorneys and industry experts are knowledgeable in how regulatory agencies work and how laws and enforcement trends have evolved and are therefore able to advise clients proactively on a wide range of issues, including promotional practices, regulatory approvals, pricing and reimbursement and product recalls. With its in-depth understanding of the commercial and regulatory aspects of these activities, Kim & Chang provides practical advice that is unmatched in Korea.

Authors

Kyungsun Kyle Choi is a foreign attorney at Kim & Chang and a member of the Mergers & Acquisitions, Corporate Investigations and White-Collar practice groups. Ms Choi represents a broad range of companies in the life sciences and digital health, medical device, food and cosmetic sectors, specialising in regulation, pricing and reimbursement, compliance, bribery and competition law issues relating to promotional and marketing practices in the industry, anti-counterfeiting strategies, M&A, and restructuring of business operations. Ms Choi's recent work has been in defending clients in the pharmaceutical industry in a wide range of internal and government investigations who face allegations of corporate fraud, corruption, fair trade law violations and bribery.

Eui Seok Kim is an attorney at Kim & Chang, practising in various groups, including the Healthcare and Mergers & Acquisitions practice groups. He represents a wide range of clients in the pharmaceutical, medical devices, IT, chemical, distribution, logistics and mobility sectors. Based on his understanding of various technologies, Mr Kim's practice includes addressing issues that may arise in the area where existing industries meet new technology. Mr Kim has been involved in numerous government and private organisations and participated in lectures and panel discussions on the subjects of digital health, mobility, AI, and privacy, among others.

Myung Soon Chung is a foreign attorney practising in Kim & Chang's Healthcare and Antitrust and Competition practice groups. Ms Chung has advised numerous multinational pharmaceutical and medical device companies on anti-bribery, regulatory requirements, pricing and reimbursement, as well as in connection with disputes with distributors. Ms Chung has also represented numerous multinational companies in cartel, fair trade and market dominance investigations, including in the pharmaceutical, medical device, paper, air carrier, commercial vehicle and IT industries. Her practice includes advising clients during disputes raised before the Korea Fair Trade Mediation Agency.



Ari Yoon is an attorney at Kim & Chang and a member of the firm's Privacy & Data Security and Healthcare practice groups. Ms Yoon has advised numerous multinational pharmaceutical, medical device, and health data companies specifically on privacy-related issues, including cloud usage, use of electronic medical records, and processing personal data of healthcare professionals' data for digital and multi-channel marketing purposes. Ms Yoon has also represented such companies in various regulatory investigations. A member of data and privacy-related academic societies, she has frequently participated in seminars on data, privacy, and personal information protection hosted by regulatory authorities and industry bodies, both as a presenter and a panellist.

Kim & Chang

39 Sajik-ro 8-gil
Jongno-gu
Seoul 03170
South Korea

Tel: +82 2 3703 1114
Fax: +82 2 737 9091/9092
Email: lawkim@kimchang.com
Web: www.kimchang.com

KIM & CHANG

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

"Digital healthcare", "digital medicine" and "digital therapeutics" refer to the integration of traditional healthcare into the digital environment. The core technologies allowing for this digital transformation include the internet of things (IoT), cloud computing, sensors, big data and artificial intelligence (AI).

Medical Data

Medical data that an individual directly or indirectly generates can largely be divided into three categories:

- genetic information;
- personal health information; and
- electronic medical records (EMRs).

With regard to genetics, an individual generates roughly three billion genetic base pairs, which allows the implementation of precision medicine, personalised new drug development, genetic editing and synthetic biology.

Personal health information refers to information that is collected through, for example, wearable devices and other healthcare-related monitoring apps (eg, blood sugar levels, blood pressure, heart activity, and dietary information).

Such information is used to provide individuals with everyday health information, which can help prevent, or even mitigate currently existing diseases.

EMRs refer to a form of digitisation of medical records which would contain, in essence, personal information, medical history, health conditions and prescription information. The digitisation of EMRs is key in identifying specific clinical results based on analysis of genetic information and personal health information and, thus, South Korea is accelerating the process of digitising previously non-digitised medical records to allow further use of real-world data to generate real-world evidence.

The Status of Digital Healthcare in South Korea

South Korea has the world's most developed 5G network and IT technology. It is also the leading country in the use of image archiving communication systems and electronic medical reports in hospitals. This makes South Korea the optimum environment for digital healthcare to flourish.

Nevertheless, compared to global counterparts, Korea's digital healthcare industry is still in its infancy. For example, Korean companies are not found on the global list of top 100 digital healthcare start-ups, based on accumulated investments. The main reason for this is the regulatory hurdles.

Typical regulatory obstacles to digital healthcare in South Korea concern:

- telemedicine;
- the use of medical information;
- cloud storage;
- genetic information for customised medical care;
- anonymisation and pseudonymisation of medical information as big data; and
- insurance reimbursement listing of digital technology.

In March 2023, the government announced the "Plan for Regulatory Innovation of Biohealth New Industry" and proposed ways to reform regulations in the "biohealth industry", including "digi-

tal health". Specific tasks related to digital health include institutionalisation of telemedicine, and improvement of the electronic medical record system.

The introduction of digital healthcare services and related products as a result of these regulatory improvements is expected to bring about a variety of changes in providing healthcare to patients as well as the relevant technology.

For example, healthcare professionals (HCPs) in Korea will be able to provide new, innovative healthcare services to patients to prevent or manage diseases, while patients will gain access to new healthcare services not bound by time or space.

As a nation with traditionally strong technological resources, the advent and development of digital healthcare is being strongly pursued by numerous IT companies, including start-ups, in Korea.

1.2 Regulatory Definition

Definition of Digital Health

As of now, there is no definition of digital health provided in local law. However, the Digital Medical Products Act, proposed by the National Assembly in March 2023, defines digital medical products as digital medical devices, digital convergence drugs, and digital medical/health support devices, and among them, digital medical devices are defined as "medical devices to which advanced technologies such as intelligent information technology, robot technology, and information and communication technology are applied, and which are used for the purpose of diagnosing and treating diseases." The Digital Medical Products Act is currently under deliberation by the National Assembly.

Definition of Digital Medicine

Currently, there is no definition of digital medicine provided in local laws. However, the term is generally used to mean providing personalised healthcare by collecting and analysing medical data. All devices used for such purposes, however, are generally categorised as medical devices (see below).

Definition of Digital Therapeutics

There is currently no definition of digital therapeutics provided in local law. However, the government takes the position that digital therapeutics is a form of "medical device", and according to the Digital Medical Products Act proposed by the National Assembly in March 2023, a "digital converged drug" is defined as a product that combines a pharmaceutical product with a digital medical device or a digital medical/health support device, and its main function is to qualify as a pharmaceutical product.

1.3 New Technologies

Artificial Intelligence and Clinical Decision Supporting Systems

One of the most important technologies enabling the growth of digital healthcare and digital medicine is the advent of AI and clinical decision supporting systems. Digital healthcare, which uses AI for example, includes the development of software which not only provides the best treatment options based on real-world data, but also helps in the diagnosis of diseases. For example, software that reviews computed tomography and magnetic resonance images identifies diseases at a much faster rate and higher accuracy.

Big Data and Genetic Analysis

Next-generation sequencing allows for the analysis of genetic information which helps predict the probability of certain diseases in individuals.

In addition to existing laparoscopic surgery, robotic medical devices are used in areas ranging from orthopaedic surgery, such as artificial joint insertion, to surgeries such as cholecystectomy.

Other key technologies include companion diagnostics, complementary diagnostics, telemedicine services, direct-to-customer digital healthcare technology and wellness products.

1.4 Emerging Legal Issues

Telemedicine Services

The Medical Services Act (MSA) generally provides that the practice of medicine must take place physically within a medical institution. Therefore, telemedicine is, in principle, prohibited in Korea. However, because of the COVID-19 pandemic, Korean health officials had temporarily allowed telemedicine to be used in Korea (eg, consultation and/or prescription of medicine via telephone counselling). Expenses relating to these telemedicine services are also reimbursable with National Health Insurance (NHI).

Based on its examination of NHI claims from February 2020 to January 2023, the Ministry of Health and Welfare (MOHW) found extensive use of telemedicine and determined public consensus favoured telemedicine and has announced the adoption of a pilot project under which non-face-to-face treatment is permissible and reimbursable with NHI starting on 1 June 2023.

Please refer to **1.5 Impact of COVID-19** for further details.

Use of Medical Data

In 2021, the government established the "My Healthway" project, an infrastructure for sharing and using personal health records. However, under the current Medical Services Act, a medical institution cannot directly provide personal medical data to a third party, even with the patient's consent, unless such provision falls under the specified exceptions. In order to address this issue, an amendment of the Medical Services Act has been proposed to introduce the "right to request the transmission of medical information to a third party" to medical institutions.

Wellness Products

Wellness products refer to everyday instruments which provide healthcare information (eg, smart watches which measure heart rates, body temperature, blood pressure, etc). However, there is controversy about which products constitute "medical devices" and therefore require marketing authorisation.

The concept of "digital medical/health support device" was introduced in the recently proposed Digital Medical Products Act. Digital medical/health support devices refer to "instruments, machinery, devices, software or other similar products designated by the MFDS to which digital technology is applied, that are not digital medical devices but are used to monitor, measure, collect, analyse, etc, biometric signals for the purpose of supporting medical services or maintaining and improving health." Products that are currently classified as wellness products and are not specially regulated may be newly subject to management under the proposed Digital Medical Products Act.

Medical Services Based on AI Technology

AI technology in this sector is generally regarded as a medical device and requires marketing authorisation, which includes approval of registration for insurance under the NHI system. However, due to the lack of clear regulations, no AI technology-based medical service has suc-

cessfully obtained the necessary approval and registration. The MFDS has recently established a Digital Health Regulatory Support Division which has raised hopes of alleviating regulatory obstacles.

1.5 Impact of COVID-19

As discussed in **1.4 Emerging Legal Issues** (Telemedicine Services) the restriction on the provision of remote healthcare was temporarily relaxed during the COVID-19 pandemic. Furthermore, the Ministry of Trade, Industry and Energy (MOTIE) also permitting Korean doctors to provide telemedicine services to Korean citizens living abroad (ie, consultation and prescriptions), via a regulatory sandbox.

Due to the downgrade of the level of seriousness of COVID-19 in Korea (from "serious" level to "alert" level as of June 2023), temporary non-face-to-face medical treatment lost its legal basis. However, a pilot project was adopted by the Health Insurance Policy Deliberation Committee and implemented starting on 1 June 2023, under which non-face-to-face medical treatment is permitted and reimbursed under the NHI system. The pilot project is based on the following three principles, which were established after a series of meetings between the MOHW and the Korea Medical Association: (i) the project will focus on returning patients, (ii) the project will focus on clinic-level medical institutions, and (iii) patients will be permitted to choose pharmacies.

Under the pilot project, patients would be limited to returning patients who have been treated in person at least once for the same disease at the same clinic. Non-face-to-face medical treatment is permitted for first-time patients only in exceptional cases where patients are in remote areas or have impaired mobility. For paediatric patients (those under the age of 18), medical consultations (but no prescriptions) are permitted at night and on holidays, even if there is no record of a face-to-face visit.

Also, under the pilot project, non-face-to-face medical treatment will be limited to clinic-level medical institutions. Hospital-level medical institutions are permitted to provide non-face-to-face medical treatment only in exceptional cases for patients with rare diseases who have had one or more face-to-face visits and whose physician determines that they need ongoing care after surgery or treatment.

Finally, the pilot project prohibits auto-assignment of pharmacies, which was a feature in the existing telemedicine platform app used during the COVID-19 pandemic. The pilot project allows patients to choose the pharmacy they want by displaying all available pharmacies based on patient location. Prescriptions, however, will need to be picked up in person with home deliveries permitted only in exceptional cases where patients are in remote areas or have impaired mobility or infectious or rare diseases.

The adoption and implementation of the pilot project indicates that the health authorities have taken a major step towards permitting telemedicine, but controversy is expected to continue. The health authorities will need to continue to maintain a consensus between the public and pharmaceutical and medical professionals.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

Key Regulatory Agencies

Ministry of Health and Welfare (MOHW)

The MOHW is a key stakeholder as the ministry in charge of the following:

- developing national healthcare policies;
- managing the fiscal sustainability of the NHI system; and
- overseeing policy implementation.

The MOHW has issued guidelines such as the Guidelines on Non-Medical Healthcare Services (which provide guidelines on which products are medical devices and which are non-medical devices) and the Guidelines for the Use of Anonymised/Pseudonymised Medical Data, among others.

Health Insurance Review and Assessment Service (HIRA)

The HIRA reviews and assesses healthcare costs and healthcare service quality and supports NHI policies in determining medical fee schedules and drug prices. HIRA is responsible for developing guidelines that apply to the insurance reimbursement listing of digital medical services and devices.

The National Health Insurance Service (NHIS)

For drugs determined to be reimbursable, the NHIS and pharmaceutical companies negotiate drug prices after HIRA evaluation. A key factor to be considered by the NHIS is the budget impact of the addition of a new drug.

Ministry of Food and Drug Safety (MFDS)

The MFDS reviews and approves pharmaceuticals and medical devices for safety, efficacy and quality, through technological review and inspection for their manufacturing and distribution. In February 2022, the MFDS established a Digital Healthcare Regulatory Support Division, which aims to manage the review and approval of digital medical devices.

Updates on Regulatory Authorities

On 16 March 2023, 15 members of the Health and Welfare Committee of the National Assembly proposed the Bill on Digital Medical Products. The key contents of the Proposed Bill are as follows:

- a new definition of digital medical products'
- the establishment of a regulatory system, (for approvals, etc) related to digital medical products;
- verification of the effectiveness of digital medical products and establishment of grounds for safety management;
- the establishment of grounds to promote the development of digital medical products and support them.

On 7 October 2022, members of the Health and Welfare Committee of the National Assembly proposed the Act on Promotion of Digital Healthcare and Promotion of Utilisation of Health and Medical Data (the "Digital Healthcare Promotion Act"). The key contents of the Digital Healthcare Promotion Act are as follows:

- a definition of the concept of digital healthcare;
- the scope, method, procedure, etc, of pseudonymisation of health and medical data are prescribed by law;
- the introduction of the right to request transmission of medical data and establishment of a management system; and

- a new regulatory sandbox specialised in digital healthcare.

On 10 February 2022, eleven members of the Trade, Industry, Energy, SMEs and Start-ups Committee of the National Assembly proposed the Bill on Fostering and Supporting the Digital Healthcare Industry. The key provisions of the proposed bill are as follows:

- a new definition of the digital healthcare industry;
- an obligation on MOTIE to develop plans to support the digital healthcare industry;
- certification for outstanding digital healthcare companies and establishment of grounds for such support; and
- grounds for overseas expansion of the digital healthcare industry.

2.2 Recent Regulatory Developments

Regulatory Sandbox Programme

Since January 2019, as part of the effort to improve the regulatory environment and to encourage the development of new technology and industries, the Ministry of Science and ICT and MOTIE have adopted a Regulatory Sandbox. If existing regulations are unclear, irrational or prohibitory, the Regulatory Sandbox allows three mechanisms to address these issues.

- First – under the "Proven Exception" provision, the Regulatory Sandbox will relax a restrictive regulation under specific conditions on scope, scale, and duration.
- Second – "Temporary Approval" allows for a market-first, evaluation-later approach.
- Third – under the "Active Administrative Interpretation" mechanism, a more relaxed interpretation of existing regulations is allowed.

For reference, the Digital Healthcare Promotion Act proposed in October 2022 newly introduces a regulatory sandbox system specialised for digital healthcare. Therefore, it is necessary to keep an eye on the current trends in the system.

Other Regulations

Other recent regulatory developments include:

- enactment of the Act on Fostering the Medical Device Industry;
- promulgation of Guidelines on Specific Plans for Use of Medical Data;
- amending the evaluation standard for innovative medical technology;
- regulations on procedures and methods for designation of innovative medical devices;
- an amendment to the Guidelines on Implementation of Innovative Medical Technologies and the Guidelines on Management of New Medical Technologies Subject to Suspended Evaluation; and
- the announcement of the Guidelines and Casebooks for Non-medical Health care Services (1st and 2nd).

2.3 Regulatory Enforcement

Regulating the Practice of Medicine

The MSA stipulates that only HCPs are permitted to conduct medical services and such HCPs may only carry out medical services for which they have licences. Providing medical services without a licence is strictly prohibited. However, the current MSA does not define "medical services", and case precedents have broadly interpreted its meaning (eg, the provision of tattoo services in Korea is deemed to be the provision of medical services).

Therefore, providing some form of (even perfunctory) diagnosis service to customers (for example, using mobile phone applications) can

be deemed as providing medical services. This has been controversial for insurance companies that have been attempting to use big data to provide consumers with a statistical analysis of their health (eg, life expectancy, chances of being diagnosed with a particular disease).

Telemedicine

The laws regulating telemedicine have been temporarily relaxed in light of the COVID-19 pandemic. However, this is only temporary and the prohibition of telemedicine under the MSA will remain after the pandemic. See **1.5 Impact of COVID-19** and **7.2 Regulatory Environment** for more details.

Prohibition of Provision of Economic Benefits to HCPs

The Pharmaceutical Affairs Act (PAA, applicable to pharmaceutical companies) and the Medical Device Act (MDA, applicable to medical device companies) both explicitly prohibit the provision of economic benefits to HCPs for the purposes of promoting sales. "Economic benefits" is interpreted broadly and, thus, providing meals or drinks (or paying for other forms of entertainment for HCPs) are deemed prohibited per the above statute.

There are attendant regulations to the PAA and MDA which provide for certain safe harbours regarding the provision of economic benefits to HCPs.

Administrative Sanction Procedure

In an administrative enforcement action, companies are provided an opportunity to present their defence before an administrative decision is rendered. Companies may also challenge the administrative decision (administrative fine, corrective order, etc) by filing a lawsuit with the administrative court under the Administrative Litigation Act, or by initiating an administrative appeal with the general court system under the Administrative Appeals Act. Companies charged with criminal violations of relevant statutes can proffer defences through the criminal trial process. The procedure for administrative cases is nearly identical to that of civil cases:

- a complaint is filed and served upon the defendant;
- arguments are made thereafter in the answer, reply brief, and other rebuttal briefs; and
- evidence is examined at hearings and a judgment is rendered.

A final decision on the matter can be, in general, expected six months to a year following the initial filing.

Liability Exemption Based on the Compliance System

Companies can be exempt from liability if they are able to prove that they had a robust compliance system, and that any wrongdoing by an individual of the company was a remote event. Such compliance measures include:

- strict internal regulations;
- rigorous oversight by the legal/compliance teams;
- emphasis on compliance by the management; and
- severe disciplinary sanctions against employees/executives who engage in wrongdoing.

Thus far, however, the Korean government has been strict in exempting companies from liability based on the existence of strong compliance systems.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

There are several other regulatory agencies involved in digital healthcare including the following:

- MOTIE, which seeks to nurture and develop new industries, such as the digital healthcare industry;
- the Ministry of Science and ICT, which seeks to further develop IT technology;
- the Korea Communications Commission, which enforces regulations on information and telecommunication services; and
- the Personal Information Protection Commission, which aims to ensure that the personal information on Korea's citizens is fully protected.

A certain tension exists between such regulatory bodies and the MOHW, whose role is to regulate the Korean healthcare sector. For example, MOTIE desires to actively incentivise and promote the digital healthcare industry, whereas the MOHW seeks to slow the process down until it is certain that any new technology is not a threat to the health of the citizens.

For instance, the Bill on Fostering and Supporting the Digital Healthcare Industry, which is currently being reviewed by the National Assembly, foresees that products/platforms used for medical services would be managed by MOTIE. At the same time, the PAA and MDA are both under the purview of MOHW and, thus, the MOHW renders the ultimate decision on whether a new digital healthcare products and/or platforms should receive marketing authorisation (if the product is deemed a medical device). Inevitably, there could be conflict between these two agencies.

Furthermore, the Ministry of Science and ICT may become a major regulatory body when it comes to healthcare technologies involving AI. On February 14, 2023, a subcommittee of the National Assembly's Science, ICT, Broadcasting, and Communications Committee passed a proposed Act on the Promotion of the AI Industry and a Framework for Establishing Trustworthy AI (the "AI Act"). The proposed AI Act designates certain types of AI used in direct connection with human life and safety as "high-risk AI", requires that such high-risk AI achieve a certain level of trustworthiness, and proposes certain notice requirements. If the AI Act is enacted, AI systems used in medical devices may be categorised as "high-risk AI" and the Ministry of Science and ICT will be another authority competent to regulate in this area.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

There are no definitions for "preventative care" or "diagnostic care" under Korean law. However, preventative care generally refers to medical check-ups (where the general health of a person is analysed to confirm/prevent any diseases), while "diagnostic care" is generally used to treat diseases where symptoms already exist.

One of the main regulatory schemes that apply to preventative/diagnostic care is the NHI system. South Korea operates a compulsory NHI system that provides coverage for all residents, and primarily comprises general health insurance and a medical aid programme for low-income families. The MOHW oversees the NHI

system and is responsible for setting healthcare policies. The MOHW also supervises the following agencies:

- the NHIS, which operates the NHI system and serves as the insurer; and
- the HIRA, which is responsible for assessing reimbursement claims submitted by medical institutions.

While the majority of Koreans subscribe to some form of private health insurance, this is in addition to the NHI system; private health insurance cannot duplicate or replace the NHI system. The NHI system provides comprehensive medical coverage for designated medical treatments.

In this regard, President Suk-Yeol Yoon's administration has made various pledges under the slogan "the State is responsible for essential medical care." Specifically, the new administration has publicly stated that the scope of the State's responsibilities in various areas of essential medical care will be expanded to include:

- securing essential medical facilities, such as emergency rooms, etc;
- mitigating public pain caused by medical expenses (regardless of the type of disease) by expanding support for catastrophic medical needs; and
- expanding various public vaccination programmes.

4.2 Increased Preventative Healthcare

Various factors have contributed to the increased use of preventative care. These include:

- the development of digital healthcare products (such as wearable devices to check daily exercise routines, glucose levels, etc);
- the increase in life expectancy and the desire for people to stay healthy throughout their lifetime;
- government promotional actives (such as advertisements and policies aimed at ending smoking); and
- overall societal understanding that preventative care would contribute to the overall cost savings for the individual and the state.

Such trends are expected to continue in the future.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Wellness and fitness data is first and foremost subject to the regulations of the Personal Information Protection Act (PIPA), which prescribes comprehensive regulations on the processing and handling of personal information. Stricter restrictions are imposed on healthcare-related data which is considered "sensitive data". Products which provide wellness and fitness data may also be deemed "medical devices" by the MDA and would, therefore, require prior marketing authorisation.

No separate laws regulate an individual's data where such data is a combination of data regulated under healthcare regulatory regimes and data regulated under another or no regulatory regime; there are, however, certain practical constraints on how such data is accessed. For example, there is no separate centralised database system where a patient's medical records from different hospitals are gathered and reviewed. There have, therefore, been discussions on establishing a national healthcare database (My HealthWay) which would collect all the medical data of individuals and allow them to access such data whenever and wherever they

wished. See **1.4 Emerging Legal Issues** (Use of Medical Data) for further discussion.

Meanwhile, as explained in **1.4 Emerging Legal Issues**, an amendment of the Medical Services Act has been proposed to introduce the "right to request the transmission of medical information to a third party" to medical institutions.

In Korea, judges and courts are not able to make laws (ie, the concept of case law does not exist in Korea). Court precedents do provide strong guidance, but no such decisions have been made with respect to digital healthcare.

4.4 Regulatory Developments

There are no current or proposed regulations specifically addressing preventative healthcare. Instead, all relevant legal issues are addressed by general laws such as the MDA, PIPA, and the Product Liability Act (PLA), etc.

Nevertheless, relevant bills such as the Digital Healthcare Promotion Act, the Digital Healthcare Promotion Act, the Digital Medical Products Act, and the AI Act are currently being reviewed by the National Assembly. Except for the AI Act, these acts seek to establish stronger legal grounds for the government's efforts to help support and foster the digital healthcare industry. For more information, please refer to **2.1 Healthcare Regulatory Industries**. For the AI Act, please refer to **3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies**.

4.5 Challenges Created by the Role of Non-healthcare Companies

Provision of Medical Services by Non-HCPs

The MSA stipulates that only HCPs are permitted to provide medical services and such HCPs may only carry out medical services for which they have licences. As explained in **2.3 Regulatory Enforcement**, providing medical services without a licence is strictly prohibited and providing some form of (even perfunctory) diagnosis services to customers (eg, on mobile phone applications) can be deemed as providing medical services.

This has been controversial matter for IT companies that attempted to use digital healthcare tools (eg, to provide consumers with a statistical analysis of their health, life expectancy, chances of being diagnosed with a particular disease). Accordingly, whenever a new digital healthcare service is developed the relevant company must be careful to ensure that the service provided is not a "medical service" as defined in the MSA.

Broad Definition of "Medical Devices"

The MDA governs the management of medical devices, including manufacturing, importation, sale and use and public health issues associated with the devices. The MDA defines "medical device" as "an instrument, machine, device, material, software, or any other similar product [...] used for the purpose of [...] diagnosing, curing, alleviating, treating or preventing a disease" in humans or animals.

As the definition is somewhat ambiguous (and without much additional detailed guidance), the MFDS tends to interpret the definition broadly. For example, the MFDS has ruled that "computer aided detection and diagnosis software" and "software that efficiently checks, analyses, transmits and prints medical images and treatment information in the field of radiation oncology" are medical devices under the MDA. The MFDS has further stated that software that assists and supports clinical decision-making by HCPs is a medical device. If a product constitutes a medical device, the company will need to

receive a market authorisation which will require, among other things, clinical trial data to be submitted to the MFDS.

Overseas Transfer of Personal Information

Numerous multinational companies with no relevant resources in Korea often require assistance from their affiliates abroad. However, the MSA provides that "[n]o one may disclose, alter, or destroy any personal information stated in an EMR without a justifiable reason". Accordingly, transferring medical records to a third party outside a medical institution is, in principle, illegal in Korea. There are exceptions, but these have very strict requirements.

Additionally, national and public medical institutions cannot store their data (eg, personal information or EMRs) overseas when using a commercial cloud computing service. National and public medical institutions must use a commercial cloud computing service that is certified under the Cloud Security Assurance Programme (CSAP), and in order to obtain such certification, the cloud system and hosted data must be physically located in Korea.

Meanwhile, under the amended PIPA, which will take effect on 15 September 2023, a personal information controller that is not an online service provider (OSP) is required to prepare procedures for overseas transfer, including the consent of the data subject, in case of overseas transfer of personal information. Consent can be waived only in the case of overseas outsourcing or storage of personal information when it is necessary for the execution and performance of an agreement with the relevant data subject. Therefore, when multinational companies transfer personal information, such as patient information, to their overseas affiliates, they must obtain separate consent for the overseas transfer, and in the case of overseas outsourcing/storing for the purpose of execution and performance of an agreement, they must disclose the details in their privacy policy, etc.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

The development of 5G, AI, machine learning and subsequent application of such technologies to wearable devices have contributed to the development of the "internet of medical things" (IoMTs). Such technologies have had a particularly strong impact on preventative medical services (eg, monitoring blood pressure, glucose levels).

The use of such products by individuals and hospitals, however, has been somewhat limited. This is because such products often constitute medical devices which would require marketing authorisation. Furthermore, the data collected by such products should be sent directly to medical institutions, which could cause regulatory issues concerning personal information protection. Such regulatory hurdles will need to be addressed in the near future to ensure innovative IoMTs can be fully utilised.

5.2 Legal Implications

If an adverse healthcare outcome is caused by a fault attributable to an HCP, the Civil Code and Criminal Code will apply. In such cases, the HCP will be liable for the harm caused to the patient and may also be subject to criminal liability if there is bodily harm and the HCP was negligent. The HCP will need to argue that they were not negligent to avoid both such liabilities.

If an adverse healthcare outcome is caused by a medical device or drug, the manufacturer of the device or drug can be held liable.

Civil Liability

According to the PLA, manufactures and sellers of products will be liable for damages caused by a "defect in a product" which is categorised as a manufacturing defect, design defect or warning defect (where sufficient warning was not provided). Under the PLA, it will be presumed that the product was defective at the time of supply and that the defect caused the damages if a victim is able to prove the following:

- damages were sustained while the product was being used normally as intended;
- the damages occurred from a cause that originated within the boundaries controlled by the manufacturer; and
- the damages would not normally occur in the absence of a defect.

A manufacturer may be exempt from product liability claims in the following circumstances:

- the manufacturer did not supply the product;
- the alleged defect could not have been discovered by scientific or technological standards available at the time the product was supplied;
- the alleged defect was caused by the manufacturer's compliance with standards mandated by laws in effect at the time the product was supplied; or
- with respect to suppliers of raw materials or parts/components, if the alleged defect was caused by the purchasing manufacturer's specifications regarding the design or manufacture.

Criminal Liability

According to the Criminal Code, the manufacturer of a medical device/drug could be criminally liable if the product causes bodily harm to the victim and the manufacturer was negligent in causing a defect which caused such bodily harm. The manufacturer in this instance will need to prove that it was not negligent.

5.3 Cybersecurity and Data Protection

All medical information stored in clouds or local computers are subject to cyber-attacks. Such risk has resulted in the growth of cybersecurity IT companies, as well as strict laws and regulations.

For example, when applying for marketing authorisation for a medical device which has telecommunication functions, strict cybersecurity protection measures are required. For example, the ISO 14971 is applied to evaluate the risk and the medical device must be capable of encrypting data when transferring such data; logs must also be created for all relevant events.

Furthermore, medical institutions must maintain strict regulations pertaining to their equipment and facilities that store and process medical data. Such requirements are more stringent when medical institutions want to store such data on servers located outside the medical institution.

5.4 Proposed Regulatory Developments

The distinction between medical devices and non-medical devices for products that provide diverse healthcare related services is still not entirely clear. For example, if a product is not just a wellness product, but rather acts to diagnose or treat diseases, the product will be categorised as a medical device, and thus, will require marketing authorisation. If the product is

not considered to be a medical device, it will only require other minor, electronics related approvals. While the government has been working to issue guidelines to make the distinction clearer, the boundaries are still quite unclear.

As described in **4.5 Challenges Created by the Role of Non-healthcare Companies**, the MSA only allows HCPs to provide medical services. Accordingly, if a particular service is not a medical service, but rather, a "wellness management service", such a service can be provided by non-HCPs outside of medical institutions. The boundaries of this distinction, however, are also unclear. The MOHW has issued guidelines to help elucidate the boundaries, but there is still much controversy.

All such issues are handled mainly by the MOHW.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

According to the Digital Treatment Devices Approval and Review Guideline, software as medical device technologies (SaMDs) are defined as:

- "a medical device that is not dependent on hardware;
- has a function that meets the intended use of the medical device; and
- consists solely of independent software".

As a medical device, the marketing authorisation and management of SaMDs are handled by the MFDS. SaMDs, as with other medical devices, are categorised into four different classes, depending on the level of risk posed to the patients by such devices.

Similarly to other medical devices, if SaMDs are upgraded to include new features or functions, additional authorisation will need to be obtained. Simple upgrades to fix bugs (or simple patch updates) will not require additional authorisation (for AI/machine learning-based SaMDs, please see below).

Whether a product uses AI and machine learning will not affect whether it falls into the category of a medical devices. For more information on the definition of medical devices, please refer to **4.5 Challenges Created by the Role of Non-healthcare Companies**. If a product uses AI/machine learning and falls into the category of a medical device, the party applying for the marketing authorisation will need to disclose the relevant algorithm.

The question arises as to whether AI/machine learning-based SaMDs require additional marketing authorisation whenever the AI/machine's functions are improved due to the machine learning feature. Currently, the MFDS takes the position that, as long as the manufacturer does not advertise such enhancements due to machine learning, a marketing authorisation amendment would not be necessary. However, if a new feature or function is added, an additional marketing authorisation amendment will be required.

The biggest hurdle faced by SaMDs is receiving NHI reimbursement. The government does not yet have a system by which to manage NHI reimbursement for SaMDs, which makes it difficult for hospitals to use such products. We are hopeful that the government will soon address this issue.

Additional requirements apply to national and public medical institutions. As mentioned in **4.5 Challenges Created by the Role of Non-healthcare Companies**, these institutions may only use commercial cloud computing services that are CSAP-certified. Therefore, if SaMDs is based on a commercial cloud computing services, only SaMDs that use CSAP-certified services would be available for these institutions. To obtain CSAP certification, the cloud service provider must meet strict requirements, such as data and personal localisation, physical separation of networks, and Common Criteria certification. These particularly strict requirements have been recognised as hindering foreign commercial cloud service providers from providing services to the national and public medical institutions.

7. Telehealth

7.1 Role of Telehealth in Healthcare

Even with the temporary relaxation of relevant regulations on telemedicine in light of the COVID-19 pandemic, the government is currently not considering permitting the operation of virtual hospitals or virtual visits to hospitals. Although such services may be allowed in the future, it is difficult to confirm when this will happen.

In the meantime, medical services to residents in Korea must be provided by HCPs licensed to practice medicine in Korea. Accordingly, it is currently not possible for foreign HCPs to provide medical services to residents in Korea. Please refer to **1.5 Impact of COVID-19** for more details.

7.2 Regulatory Environment

While the COVID-19 pandemic has caused the government to relax regulations regarding telemedicine, it is (as of now) only a temporary measure.

The proposed amendment to the Medical Services Act, which allows non-face-to-face treatment, was submitted to the Subcommittee on the Review of Bills of the Health and Welfare Committee of the National Assembly in April 2023, but was not passed (five amendments to the Medical Services Act that stipulate the institutionalisation of non-face-to-face treatment and one amendment to the Medical Services Act that regulates non-face-to-face treatment brokerage platforms were reviewed together). The National Assembly commented to the MOHW to come up with countermeasures, pointing out the possibility of commercialisation of medical care, institutionalisation of pharmaceutical delivery, issuing of public electronic prescriptions, whether to introduce prescriptions for ingredients, and the fact that the number of non-face-to-face treatments has not been resolved at all.

However, the MOHW has adopted and implemented a pilot project, which began on 1 June 2023, and under which non-face-to-face medical treatment is permitted to a certain extent because the previous legal basis for the temporary non-face-to-face treatment disappeared due to the loosening of COVID-19 restrictions.

Please refer to **1.5 Impact of COVID-19** for further details.

7.3 Payment and Reimbursement

The MSA prohibits telemedicine offered directly from medical personnel to patients. On 15 December 2020, the Act on Prevention and Management of Infectious Diseases was amended to temporarily allow HCPs to provide telemedicine to patients under certain specific circumstances due to the COVID-19 pandemic. This temporarily permitted telemedicine lost its legal basis as COVID-19 restrictions were loosened, but a pilot project was adopted and implemented on 1

June 2023 permitting non-face-to-face medical treatment to a certain extent. This pilot project allows HCPs to use information and communication technologies such as wired, wireless, video communications and computers to continuously observe, diagnose, examine and provide medical services to patients outside medical institutions.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

IoMTs are integrated software, devices, hardware, etc, that help HCPs monitor patients or diagnose or treat diseases. The main technology used for IoMT includes 5G networks, big data analysis, and AI.

The most important legal issues faced by IoMTs include the following.

- Medical devices – depending on what information is being collected and analysed by IoMTs, the relevant product could be categorised as a "medical device", which would then require prior marketing authorisation.
- Provision of Medical Services – depending on what services are being provided by IoMTs (eg, analysing blood pressure, glucose level), such products could be considered to be providing medical services. This could be a violation of the MSA, as the MSA prescribes that only licensed HCPs can provide medical services.
- Personal Information – manufacturers of IoMTs must ensure that all personal information collected via the relevant products is collected in a manner that is compliant with the data privacy laws in Korea.

Meanwhile, since the recent launch of ChatGPT, various "digital assistant" services that provide medical information have been launched or are shortly to be launched in Korea. However, such services may constitute "medical practice by non-medical personnel" prohibited by the MSA.

Therefore, the digital assistant service should be limited to simply introducing materials such as standard medical guidelines that have already been disclosed, and in order to reduce the risk of violating the Medical Services Act, the service providers are advised to add a clear disclaimer to the effect that "specific medical information should be inquired of HCPs."

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

Impact of 5G Networks

Since the first commercialisation of 5G networks in the world in April 2019, Korea has been rapidly distributing 5G networks. As a result, many changes are expected to take place in the digital healthcare market in Korea.

The 5G network infrastructure is spreading relatively quickly in Korea, setting the foundation for a rapid change in the digital healthcare market. The government plans to complete the establishment of 5G networks including rural areas by 2024. In addition, the government is planning to lead the 5G network era by establishing a specialised network that provides 5G services customised to the needs of various industries, including medical services.

In addition to the spread of the IoT, 5G is also bringing about many changes in hospitals. In Korea, mobile carriers (companies that pro-

vide mobile phone communication services) and hospitals are working together to build 5G smart hospitals that incorporate AI and immersive content.

More specifically, AI speakers have been installed in hospital rooms and attempts are being made to monitor patients' biological signs comprehensively with online hospital visits by patient's caregivers, ward dashboards and mobile devices using immersive media technologies such as holograms. Also, informatisation of medical records through AI voice recording, virtual reality nursing practice, management of the location and usage of dangerous drugs based on IoT, virtual reality healing for patients with limited mobility, and IoT hospital rooms that promote stable sleep and provide air quality checks, are being implemented.

The government has implemented 5G services in ambulances, enabling rapid data transmission between ambulances and a cloud-based platform that analyses patient information and provides instructions on first aid and hospital selection during patient transport.

5G is also making the establishment of mobile hospital infrastructures that can be used in disaster areas, etc, a reality. In May 2021, the government announced its plan to create the world's first mobile hospital to expand healthcare services to underprivileged areas, such as disaster areas, using AI diagnostic equipment based on 5G technology. Under the plan, the government expects to develop mobile hospitals that can be operational within sixty minutes in disaster situations or in vulnerable areas.

Commercial and Contractual Considerations

Although Korea's 5G network infrastructure environment is excellent, there are still strict regulations on certain areas with regard to digital healthcare. Therefore, it is necessary to first review whether the services to be provided are available and how the regulations could be relaxed accordingly.

In addition, even if it is difficult under the current regulations, it is necessary to examine whether the temporary permit, based on a de-regulatory sandbox system (ie, a safe harbour where companies can freely experiment new ideas and technologies, as children do with their toys in a sandbox) which was adopted in January 2019 in Korea, can be used to provide services before the regulations are relaxed.

Furthermore, it is important to clarify who would be responsible for the various licences/permits and who would be responsible for information security failures, such as the leakage of personal or medical information, etc, in executing contracts between partners such as mobile carriers and hospitals.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

The collection, use and provision of personal health information may be subject to the PIPA, the MSA, and the Bioethics and Safety Act (BSA). Although the PIPA is a general law governing the processing of personal information, the MSA takes precedence over the PIPA for patient records held by medical institutions, and the BSA takes precedence over the PIPA for research on human subjects including clinical trials. In the following sections, we will explain the collection, use and provision of personal health information under the PIPA, MSA and the BSA.

Personal Information Under the PIPA

As mentioned above, the PIPA is a general law governing the collection, use and provision of personal information. Therefore, the PIPA is applicable unless other laws and regulations specifically provide for the processing of personal information.

Personal information, which is regulated by the PIPA, refers to information pertaining to a living individual that (i) can be used to identify an individual, or (ii) can be easily combined with other information to identify an individual even if such information in and of itself cannot identify the individual.

In principle, consent from data subjects is required to collect, use and provide personal information. Personal information includes not only general personal information, but also health-related sensitive information. Consent to use sensitive information should be obtained separately from other personal information. In addition, consent to the collection and use of personal information and consent to the provision of personal information to a third party must be separately obtained.

On the other hand, information that can no longer be used to identify an individual by using other information is referred to as "anonymous information," which is not subject to the PIPA.

Pseudonymised information refers to information that cannot identify a particular individual without the use or combination of additional information to restore the original identity of the subject. Such pseudonymised information is regulated by the PIPA, but unlike other personal information, it may be used for the purpose of compiling statistics, conducting scientific research and preserving records for the public interest, without the consent of the data subject. This concept of "pseudonymised information" was recently introduced due to the need to use information in various fields including digital healthcare.

Digital Healthcare and Pseudonymised Information

To collect, use and provide personal information (which is not pseudonymised), individual consent from the data subject is required. However, in the case of pseudonymised information, if it is used for the purpose of compiling statistics, conducting scientific research, preserving records for the public interest, etc, it can be processed without the data subject's consent. As the need to use information for research and other purposes is increasing, the use of pseudonymised information is increasing due to the difficulty of obtaining consent from data subjects.

The Personal Information Protection Committee and the MOHW have collectively published the "Guideline on Utilisation of Healthcare Data" to explain the standards, methods and procedures for pseudonymisation of individual healthcare data. For example, in the case of image information such as endoscopy, X-ray and ultrasound, if an identifier (eg, patient number or name) is deleted or masked and the Digital Imaging and Communications in Medicine (DICOM) header is deleted from the metadata, such information may be regarded as pseudonymised information.

However, the PIPA provides that pseudonymised information should not be processed for the purpose of identifying a specific individual. As information processed for personalised treatment, diagnosis, etc is subject to restoration/re-identification, it is difficult to regard such information as pseudonymised information.

Fields Subject to the MSA and BSA

The MSA takes precedence over the PIPA with respect to the records of patients held by medical institutions. In particular, if a medical institution is required to provide a third party with access to (or a copy of) the patient's records, the MSA applies. Patient records may be provided to a third party only when they meet the strict requirements under the MSA. However, the Guidelines for Utilisation of Healthcare Data explain that the PIPA, not the MSA, applies to medical records and pseudonymised information that cannot be used to identify a specific patient. Thus, institutions may consider using pseudonymisation when using such medical records/information for digital healthcare.

The BSA applies to studies on human subjects, including clinical studies. Under the BSA, a researcher may provide personal information after deliberation by the Institutional Review Board if the researcher obtains written consent from the data subject.

In addition, in order to provide such personal information to a third party:

- all or part of the personally identifiable information must be replaced with the relevant agency's unique identification code; or
- consent to the provision of personal identifiable information from the data subject must be obtained.

Leakage of Personal Information

Regulations on personal information leakage and data breach are set forth in the PIPA. If personal information is leaked due to a failure to take necessary measures to ensure the safety of the information, imprisonment of up to two years or a fine of up to KRW20 million may be imposed on the violator. In addition, an administrative fine of up to 3% of the sales related to the violation may be imposed if the personal information processor is an IT service provider (digital healthcare is likely to fall into this category).

However, under the amended PIPA, which will take effect on 15 September 2023, the criminal sanctions will be abolished. Instead, the violator may be subject to an administrative fine not exceeding 3% of the total revenue (less the revenue unrelated to the violation), unless the violator has fully implemented the required measures to prevent leakage of personal information.

On the other hand, a data subject may claim for damages if they have suffered injury due to the personal information processor's leakage (if it is difficult to specify the specific amount of damages, they may claim for up to KRW3 million). If personal information is leaked due to wilful misconduct or gross negligence of the personal information processor, the processor may be held liable for punitive damages of up to three times the amount of damages to the data subject. Under the amended PIPA, punitive damages are increased to up to five times the amount of damages to the data subject.

Meanwhile, in relation to the fields covered by the MSA, if an HCP divulges another person's information that they have obtained in the course of performing their duties or violates the restrictions on the provision of such information to a third party, they may be subject to imprisonment of up to three years or a fine of up to KRW30 million. However, the violator cannot be punished if no complaint is filed.

In addition, in fields covered by the BSA, a person who divulges or misappropriates confidential information may be subject to imprisonment for up to three years (a corporation or

representative may be subject to a fine of up to KRW50 million pursuant to the vicarious liability provision), and a person who provides treatment information, including genetic information, to a third party may be subject to imprisonment of up to two years or a fine of up to KRW30 million.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

The Concept of AI

There is no formalised agreement on whether AI in the healthcare sector refers to "Artificial Intelligence" or "Augmented Intelligence." However, as AI is used to support and assist HCPs in making decisions on medical treatment, prescription and medication, it is reasonable to view it in the healthcare sector as "Augmented Intelligence" rather than "Artificial Intelligence".

Utilisation of Personal Health Information for the Development of Machine Learning Algorithms

The collection, use and provision of personal information through machine learning algorithms are no different from the collection, use, and provision of personal information described in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**. Accordingly, under the PIPA, in order to collect, use and provide personal information that is not pseudonymised, consent from the data subject must be obtained.

In the case of pseudonymised information, if it is used for the purpose of compiling statistical data, conducting scientific research, preserving records for public interest, etc, it may be processed without the consent of the data subject.

When collecting information through machine learning algorithms, it will be difficult to obtain individual consent from the data subject. Therefore, whether the pseudonymised information can be collected and used would be the key issue.

In general, machine learning in the healthcare industry is used for the following purposes:

- medical and health institutions – to diagnose, predict, and treat patients' diseases and identify and predict the spread of infectious diseases;
- pharmaceutical companies – to improve the efficacy and accuracy of the new drug development process; and
- medical device companies – to develop various diagnostic systems and support personal healthcare services.

Of course, its functions are not limited to the above-mentioned categories, and it may be used for various other purposes.

Risk of Cyber-Attacks and Misuse/Abuse of Sensitive Information

Personal health information constitutes sensitive information and may be vulnerable to misuse and cyber-attacks. In particular, medical information retained by medical institutions may be used for various purposes, and there is a risk that such sensitive information could be hacked. For this reason, the MSA requires that the MOHW be notified when medical information is leaked due to electronic infringement of medical records.

In addition, personal genetic information may be at risk of misuse and cyber-attacks because such information may contain information about not only specific individuals, but also third parties such as their parents, ancestors, siblings,

descendants and other relatives. For these reasons, the Guidelines for the Utilisation of Healthcare Data provide stricter limitations on the pseudonymisation of genomic information.

Centralised Electronic Health Record Computer System

In Korea, due to the lack of standardisation of EMRs, the utilisation rate of EMRs by medical institutions is low. Accordingly, the MOHW is pursuing a project to standardise EMRs in hospitals and clinics, but the project has not yet achieved any notable results. If a standardised EMR system is implemented, medical data scattered across individual medical institutions can be utilised to the full extent permitted by law. Consequently, the quality of medical data could be improved at a national level and the pharmaceutical and medical device industries could also be developed.

Natural Language Processing and the Healthcare Field

Natural language processing is understood to be AI that helps computers understand, interpret and manipulate human languages. In the field of healthcare, it will be essential in processing and analysing various physicians' handwritten records, prescriptions, clinical trial data and image/voice data. The development of AI with natural language processing capabilities will make it possible to use personal healthcare information for various purposes as explained earlier in this section.

11.2 AI and Machine Learning Data Under Privacy Regulations

The amended PIPA introduces the right of data subjects to refuse or request an explanation of decisions made through the processing of personal information via a fully automated system (including systems applying AI technology) if such automated decision significantly affects the rights or obligations of the data subject. This provision, which will enter into force on 15 March 2024, is similar to Article 22 of the EU's General Data Protection Regulation (GDPR).

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

The biggest hurdle faced by companies developing new digital healthcare technologies is the slow-changing regulatory environment. Because many of the innovative digital technologies are not permitted under the current laws and regulations (or fall into grey areas), many such companies are not able to aggressively invest in new, innovative technologies.

This issue becomes particularly apparent with technology companies that seek to engage in the digital healthcare industry, but have not previously done so (ie, they lack experience regarding the regulatory environment). Accordingly, such companies often times work in co-operation with existing medical institutions, or acquire other medical device companies, etc.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

In order for a medical institution to support digital healthcare, including the fields of telehealth, machine learning, the IoT and data transmission, the institution needs to digitise and store medical records using cloud services, depending on the type of service.

In this regard, the Korean government introduced an EMR system certification in 2020 so

that medical data of hospitals can be stored in cloud services.

EMR certification is divided into "product certification" of the EMR system, granted to self-developed or commercial software products of medical institutions utilising medical data, and "certification of use" granted to medical institutions adopting such software. Medical institutions can efficiently operate the EMR system by obtaining the certification and using cloud services that meet the EMR certification requirements instead of their own IT facilities.

13.2 Data Management and Regulatory Impact

The EMR certification standard verifies whether:

- the network access in the management area of the cloud computing service providers, the service area of users, and the service area between users are separated;
- a dualised network (line, internal network configuration route, router, etc) for each section of the network is configured so that services can be provided without interruption;
- the product meets the requirements of the National Intelligence Service, such as Common Criteria certification, when introducing a product with information protection and security functions; and
- the physical location of the EMR system and its backup equipment is limited to Korea.

Some in the industry are of the opinion that these requirements should be relaxed, but the government has not announced any specific intention to do so. It remains to be seen whether these requirements will be relaxed in the future.

14. Intellectual Property

14.1 Scope of Protection

Digital healthcare is an area where medical information and IT are combined and where issues regarding patents, copyright and trade secrets can intersect.

If a device or method that provides digital healthcare is defined as an invention it can be protected by a patent. In addition, software or computer programs are often used in digital healthcare technology. Although business methods and processes may be protected through patents, the software itself may be protected by copyright from the date of creation.

Alternatively, if the owner of the information or data does not want it to be disclosed, they may wish to protect it as a trade secret. Information may be protected as a trade secret as long as the following requirements are met:

- it is of a non-public nature;
- secrecy is maintained; and
- it has useful economic value.

In the case of data and databases used in machine learning, these can be protected as compilation works under the Copyright Act or as trade secrets. Moreover, the recent amendment to the Unfair Competition Prevention and Trade Secret Protection Act has additionally listed an act of unfairly using or disclosing another person's data as an act of unfair competition. Thus, it is possible to seek remedy under the above Act.

Currently, there is a global controversy over the ownership of inventions created by AI and whether patents should be granted for those inventions, with countries having differing opin-

ions. However, most countries are taking the position of not recognising AI inventions since an AI is not a "natural person." Korea is taking a similar position.

14.2 Advantages and Disadvantages of Protections

Since patents, trade secrets, and copyrights are the main issues in the field of digital healthcare, the how to obtain IP rights, the protection period and enforcement are explained below.

Obtaining IP Rights

Patents need to be separately registered through filing a patent application.

Trade secrets do not need to be filed but must meet the following three requirements:

- be non-public in nature;
- maintain secrecy; and
- be of economic value (Article 2, subparagraph 2 of the UCPA).

Copyright protection is available from the time of creation, without the need for any separate registration process, although it is recommended to obtain copyright for enforcement purposes.

Protection Period

The protection periods are as follows:

- patent – 20 years from the filing date of a patent application;
- trade secret – no time restrictions as long as the secrecy is maintained; and
- copyright – 70 years after the author's death (in the case of work made for hire or 70 years after publication).

Enforcement

For products and devices that can be reverse engineered, trade secrets offer little protection. In this case, it would be preferable to seek patent protection. On the other hand, for manufacturing processes where it may be difficult to prove infringement, it may be desirable to obtain trade secret protection. Copyright has the advantage of being protected without the need for any separate registration process. However, the scope of rights for a copyright tend to be narrowly construed, and if there is no intent to infringe, such as an accidental matching of expressions, there is no infringement.

Court Decision

There was a case involving a service contract for developing a picture archiving and communication system. After the contract was terminated, the service provider illegally obtained the program source code owned by the contractor. In this case, the court ruled that there had been copyright infringement and misappropriation of trade secrets.

14.3 Licensing Structures

In addition to the intersection of IP rights in digital healthcare, multiple IP owners may be involved. Thus, each of the IP rights and each owner involved should be identified in advance of making a licence agreement. Thereafter, it is necessary to set the licence scope tailored to the characteristics of each IP right and to set a separate licence agreement(s) with each owner.

If the digital technology is the result of a joint development, there are legal and practical restrictions on transfer, pledge, licensing, etc. Thus, it is desirable to reflect these in the licence agreement. Moreover, if medical data needs to be used, strict privacy issues must be addressed.

Thus, it is advisable to check whether there are any restrictions on the use of such data.

14.4 Research in Academic Institutions

According to the Invention Promotion Act of Korea, if an HCP/inventor invents an item, the right to the invention is inherently vested in the inventor, provided, however, that university or healthcare institution may acquire the right to the invention by contract or employment rules. Most university or healthcare institutions have contracts or employment rules providing for the assignment of an invention to the employer.

There are occasions where one inventor belongs to university and healthcare institutions at the same time and, in principle, the ownership of rights is determined based on the interpretation of the relevant contract.

In case of a joint development agreement, it can generally be divided into (i) research conducted with government funding, and (ii) research conducted without any government funding. In the case of government funding-based research, relevant government ministries usually provide standard guidelines on the ownership of IP rights, but in the case of a joint development, they generally require ownership sharing.

In the case of joint research by private entities, it may differ on a case-by-case basis, depending on the specific terms of the agreement. Usually, private companies want to have sole ownership of inventions coming out of R&D, but in some cases companies may share inventions in consideration of good long-term relationships (such as with doctors or professors).

14.5 Contracts and Collaborative Developments

In the case of IP rights arising as a result of joint development, there is a provision directly regulating the co-ownership relationship both in the Patent Act and the Copyright Act. However, in the case of trade secrets, there is no relevant statutory provision, but there are principles recognised in the practice as explained below. Therefore, it is necessary to keep these issues in mind when executing the relevant agreement.

Patent

A co-owner may use a patented invention without the consent of the other co-owners, but the consent of the other co-owners is required for a share transfer or pledge (Article 99 of the Patent Act). Moreover, for in service inventions, legally the default is that ownership of the invention resides with the inventor. Thus, transfer of ownership agreements is needed.

Trade Secrets

Trade secrets may be used without the consent of other co-owners. However, the consent of co-owners is required in the event of a share transfer or pledge (there is no separate provision but the co-ownership provision under the Civil Act has been applied in court precedents).

Copyright

The copyright of a joint work can be exercised only with the agreement of all the other co-owners. Any transfer or pledge of shares requires the consent of the other joint authors and the profits from the use of a joint work shall be distributed according to the degree of contribution to the joint creation (Article 48 of the Copyright Act).

15. Liability

15.1 Patient Care

There are no specific theories being discussed pertaining to liabilities arising from decisions based on digital health technologies.

The primary party liable to damages incurred to patients would be the HCPs. If the HCPs are able to prove that they did not intentionally (or by negligence) cause damages to patients, such HCPs would not be responsible for the damages caused. Whether HCPs would be considered to be "negligent" if they had engaged in treatment based on information provided by AIs is a legal area that needs to be further researched.

If, however, the digital health technology in question has a fault, then the manufacturer of such technology could be liable to the patients, according to the PLA (which levies strict liability on manufacturers of products).

15.2 Commercial

There are no specific laws which address the liability of third-party vendor's products or services that cause harm to healthcare institutions in the context of supply chain disruptions or as a vector for cybersecurity attacks, etc. Any civil liability, for example, would be addressed primarily by the Civil Code (eg, if a party defaults on its obligations to a contract, that party would compensate for the damages). It should be noted, however, that the scope of such liability can (in principle) be limited by the terms of the agreement between such parties.

SWITZERLAND

Law and Practice

Contributed by:
David Vasella and Anne-Catherine Cardinaux
Walder Wyss Ltd

Contents

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today the firm has more than 250 legal experts in six offices in Switzerland's economic centres. It is fully integrated, adapts to clients quickly, and does not hide behind formalism. Walder Wyss Ltd is the first large Swiss firm with a strong focus on tech, including data protection. Its team is familiar with recent developments not only on an academic level but also with hands-on experience from a wide range of projects. Its health sector clients represent all relevant stakeholder groups – pharmaceutical, biotech and medtech companies (including start-ups in early-stage development phases), service providers ranging from individually practising physicians to large hospital and pharmacy groups, clinical research organisations, and health insurers. Its data and technology lawyers share the same team with their healthcare and life sciences colleagues, enabling the firm to quickly navigate the cross-sectional topic of digital healthcare.

Authors

David Vasella is a partner and co-head of Walder Wyss Ltd's regulated markets, competition, tech and IP team. He advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. David deals with cross-jurisdictional data protection projects, including GDPR implementation, data retention, e-discovery, cloud projects, digital marketing, online regulation, information technology and e-business matters. He also regularly advises in relation to commercial IP matters, regulated products and market practices. In addition, he frequently speaks and publishes in his areas of expertise. David is an editor of the Swiss journal for data law and information security, is CIPP/E certified, and is a member of the professional bodies IAPP and DGRI.

Anne-Catherine Cardinaux is an associate in Walder Wyss Ltd's regulated markets, competition, tech and IP team. She advises and represents clients in all areas of constitutional and administrative law and specialises in life sciences and health law. Recently, she advised on the health law requirements for cloud projects and assessed the implications of health apps qualifying as medical devices. Prior to joining Walder Wyss Ltd, she worked as a postgraduate in the legal department at the Basel headquarters of one of the world's largest pharmaceutical companies, as a law clerk at a Zurich district court and as a junior associate in the M&A team of a leading Swiss commercial law firm in Zurich.

Walder Wyss Ltd

Seefeldstrasse 123
PO Box
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss attorneys at law

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Digital Healthcare as an Umbrella Term

The term "digital healthcare" or alternative notions of "electronic health services" and "Health 2.0" generally represent the sum of information technologies designed to increase the health, well-being or fitness of a given population or the efficiency of healthcare services – eg, by facilitating communication between healthcare providers (HCPs), healthcare organisations (HCOs) and patients. "Digital medicine" or "digital therapeutics" describes diagnostic, preventative or therapeutic attributes of information technologies. Digital medicine can thus be read as a subcategory of digital healthcare. The two terms are used in this article in this sense; "digital healthcare" will also cover digital medicine applications.

Differences Between Digital Healthcare and Digital Medicine

From a patient's perspective, digital healthcare technologies often encompass applications that generally inform about human health conditions, enable communication with HCPs, or are intended to increase patients' general well-being – eg, by encouraging an active lifestyle – whereas technologies belonging to the digital medicine realm will make claims of preventing, diagnosing or treating a human disease and improving the patient's medical condition.

From an HCP's perspective, digital healthcare primarily involves applications that increase service efficiency, such as teleconsultation or administrative case-management platforms, patient records or systems supporting the discovery of new therapies; while digital medicine applications form the object of, or influence, their medical decision-making and are subject to a corresponding duty of care.

From a regulatory perspective, digital medicine faces more stringent evidentiary requirements for substantiating medical claims and generally requires some form of clinical evaluation to be marketable in Switzerland.

Promises of Digital Healthcare

Besides improving access to healthcare and reducing inefficiencies, one of the promises of digital healthcare technologies lies in their ability to collect real-time data that can facilitate the generation of evidence required to inform medical decision-making. However, as in other

sectors, decision-making based on "real-time" or "real-world" evidence has pitfalls – using unfiltered data collected from use may perpetuate system bias and pose privacy concerns – risks that are only partly addressed in current Swiss regulation.

1.2 Regulatory Definition

Neither the notion of digital healthcare nor the term digital medicine is currently defined under Swiss regulatory frameworks.

No Comprehensive Regime

There is no comprehensive Swiss legislation on digital healthcare or digital medicine. Rather, aspects of health-related information technologies are generally qualified under each regulatory regime in view of each regulation's objectives.

Swiss legislation has a "technologically neutral" approach. Swiss laws only rarely address a specific technology. Depending on their functions, features and claims, digital healthcare and digital medicine may, for example, be subject to:

- professional practice and licensing requirements;
- provisions on therapeutic and diagnostic products;
- data protection and professional secrecy obligations;
- human (clinical or non-interventional) trial regulations;
- genetic testing legislation;
- laws on patient records;
- advertising restrictions;
- rules on the provision of benefits to HCPs, HCOs or patient organisations;
- (product-)liability regimes;
- telecommunications regulations; and/or
- public procurement provisions.

"eHealth" and "mHealth"

In 2018, the Swiss federal and cantonal administrations jointly adopted a "Swiss eHealth Strategy 2.0", where the terms "eHealth" and "mHealth" were defined. The strategy accompanied the roll-out of the electronic patient record (EPD). The term "eHealth" covers "all electronic health services that serve to network the actors in the health system". The current Strategy 2.0 draws on a previous "eHealth strategy Switzerland", which had led to the "mHealth recommendations" (dated March 2017). These recommendations define "mHealth" as "medical procedures, healthcare and preventative measures supported by wirelessly connected devices". Although the strategies and recommendations offer useful guidance, they have no regulatory qualification.

1.3 New Technologies

Digital healthcare and digital medicine are fuelled by general access to mobile devices equipped with high computing power and storage capacity, enabling real-time collection and processing of health-related data.

With increased connectivity, including wirelessly connected things (internet of things), the idea of healthcare ecosystems tailored to specific indications or conditions (such as diabetes, cardiac issues and depression) – designed to follow the entire treatment cycle from prevention and prediction to diagnosis, treatment, adherence and monitoring – is gaining momentum.

Concurrently, innovation is driven by increasingly sophisticated machine-learning and pattern-recognition technologies. Coupled with advances in genetic sequencing technologies, digital medicine applications promise to provide care tailored to an individual's genetic or physiological make-up and/or to increase diagnostic accuracy. Machine-learning algorithms in digital

healthcare technologies are used to identify new therapy candidates or improve patient triage efficiency.

1.4 Emerging Legal Issues

Important emerging legal issues in digital health include:

- cybersecurity/data protection;
- the limits of medical device and health profession regulation;
- cross-border provision of care;
- product liability for machine learning-enabled devices; and
- the reimbursement of new technologies under the mandatory social health insurance scheme.

In this cross-sectional matter, it is even more important to harmonise different regulations and ensure uniform practice. However, the legal landscape in the Swiss healthcare sector is characterised by high complexity in a field with many different players and responsibilities at all federal levels. The Swiss federal system (see **2.1 Healthcare Regulatory Agencies**) leads to a decentralised approach. This is amplified by health regulations that are not tailored to (or that are falling behind) digital health technologies.

There has been no holistic approach to healthcare data management either. Switzerland lacks a coherent and efficient environment for the lawful and secure further use of health data (see **2.2 Recent Regulatory Developments**).

1.5 Impact of COVID-19

Already in 2018 (two years before the outbreak of COVID-19), Switzerland ranked only 14th in the Digital Health Index, in a study by the Bertelsmann Foundation (a total of 17 EU and OECD countries were compared).

With the outbreak of the COVID-19 pandemic in February 2020, existing deficiencies in Switzerland's digitalisation became visible. Numerous shortcomings have been identified in the management of the COVID-19 pandemic, with the most obvious being that indicators needed to make decisions were incomplete.

In January 2022, the Federal Office of Public Health published a report on improving data management in the health sector. The report highlighted the measures that had been implemented during the pandemic and the areas where deficiencies still exist. Various national projects have followed the January 2022 report on improving data management in the health sector in the areas of health data, secondary use and data spaces (see **2.2 Recent Regulatory Developments**).

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

Switzerland is a federation with 26 states (cantons), one federal government and four official languages. The federal government is responsible for health insurance, medicines, medical devices and public health, among other things. The cantons are responsible for hospital planning or the licensing of service providers, and have a high level of competence for the organisation of their own healthcare system. By default, the cantonal health authorities implement and enforce not only cantonal but also national (health) laws.

Inter alia, Swiss cantonal health authorities have authority over medical professional practice and are competent to enforce professional licensing requirements. Their oversight touches upon digital health technologies that directly impact

on professional practice, such as platforms for telemedical services, and raises questions on the distinction between the provision of medical professional care and platforms acting as intermediaries to that care.

Swiss cantonal authorities are also competent by default to enforce the Swiss Therapeutic Products Act (TPA) governing medicinal products, medical devices and therapies directly linked to medicinal products or medical devices – eg, gene therapies. The cantonal competences under the TPA are superseded where the TPA accords express authority to the Swiss Federal Agency for Therapeutic Products (Swissmedic). Inter alia, Swissmedic is competent for market surveillance of medical devices and has authority over the marketability of medical devices. Digital medicine applications classified as medical devices within the meaning of the TPA may thus fall under both Swissmedic's and cantonal authorities' oversight.

Along with regional ethics committees, Swissmedic is also responsible for authorising certain categories of human (interventional) clinical trials with medical devices under the Swiss Clinical Trials Ordinance (eg, medical devices not yet bearing a conformity marking under medical devices regulations). Non-interventional studies with human subjects, including personal data, require an authorisation by the competent ethics committee under the Swiss Federal Human Research Act (HRA).

Swissmedic's and the cantonal authorities' competences under the TPA are complemented by competences of the Swiss Federal Office of Public Health (FOPH). Inter alia, the FOPH is also competent for granting certain authorisations under the Federal Act on Human Genetic Testing (HGTA) and for assessing the benefits of candidates for reimbursement under the general mandatory Swiss health insurance scheme.

2.2 Recent Regulatory Developments

To keep pace with evolving technologies in digital healthcare, the Swiss regulatory landscape is changing, in terms of substantive legal regimes and in the way in which regulatory authorities conduct market-surveillance activities.

Substantive Reform

In terms of substantive regimes, reforms are ongoing in patient records legislation, medical-device regulations, genetic testing and data protection laws.

Electronic patient dossier

In view of facilitating interoperability between HCPs, HCOs and digital healthcare applications, and with the aim of breaking up information silos, the Swiss legislature and regulators laid grounds for an electronic patient dossier (EPD) in 2017. The EPD is at the heart of the Swiss eHealth Strategy 2.0 and designed to integrate information derived from patient files kept by HCPs and HCOs, information entered by the patient, and mHealth applications connected to the records (see the definition of mHealth under **1.2 Regulatory Definition**). It functions as an overarching link between, and a gateway to, patient information stored locally on decentralised filing systems operated by certified EPD providers. Out of the more than 400 technical and organisational certification requirements, over 100 relate to data protection and data security. The EPD was rolled out gradually in the course of 2021.

Since 1 January 2022 (when health insurance legislation was changed) outpatient service providers must also join the EPD if they wish to provide services that are covered by mandatory health insurance.

For patients, the use of the EPD remains voluntary. They must give their consent with a two-factor authentication.

On 27 April 2022, the Federal Council informed the public that the EPD was to be developed further. It shall become an instrument of mandatory health insurance. All health professionals working in outpatient care shall be obliged to maintain an EPD. The Federal Council also plans access for research purposes with the consent of the persons concerned. It should also be possible to use the technical infrastructure of the EPD for additional services.

Medical devices ordinances

On 26 May 2021, the revised Medical Devices Ordinance (MedDO) entered into force; and on 26 May 2022 the new Ordinance on In Vitro Diagnostic Medical Devices (IvDO) also came into effect. This revision harmonised the Swiss regime with EU Regulations (EU) 2017/745 (MDR) and (EU) 2017/746 (IVDR).

Under the old regulations (the European MDD and old Swiss MedDO), and due to the mutual recognition agreement (MRA), medical devices that were placed on the market in Switzerland could be marketed in Europe with no barriers, and vice versa. However, the MRA has not been updated in line with the new regulations.

Switzerland is now a third country within the meaning of the MDR, and mutual recognition no longer exists. To access the EU market, Swiss manufacturers must designate an authorised representative domiciled in an EU member state (EU-Rep) and arrange for their devices to be placed on the market by an EU importer. According to the industry association "Swiss MedTech", efforts to meet third-country requirements will lead to initial costs representing 2% and yearly costs representing 1.4% of the total export volume.

The status as a third country also has major implications for market surveillance in Switzerland. Since Swissmedic lost access to EUDAMED, manufacturers, authorised representatives and importers must register with Swissmedic and request a "Swiss Single Registration Number", or CHRN, similar to the SRN in Europe. This is to ensure a market surveillance system in Switzerland. In future, devices will also need to be registered via Swissmedic. The deadlines and details for device registration have not yet been established. A system similar to EUDAMED is currently being set up in Switzerland.

For all other aspects, the Swiss medical device regulation remains closely intertwined with the MDR.

mHealth recommendations

mHealth applications (see the definition under **1.2 Regulatory Definition**) not falling under the regime on medical devices (eg, wearable sensors measuring vital parameters for fitness purposes) are subject to generic, non-healthcare-specific regimes on product safety. In view of addressing health-related risks inherent to mHealth applications, the Swiss regulators adopted recommendations and guidance for a self-declaration of mHealth apps based on quality criteria endorsed by the Swiss eHealth initiative. Both recommendations and guidance are designed as non-binding codes of practice increasing transparency and furthering the development of adequate quality standards.

Reform of data protection legislation

To account for the increased role and value of collecting and processing personal data, the Swiss legislature adopted a reformed Federal

Data Protection Act (FDPA), and a new Ordinance to the Federal Act on Data Protection (FDPO). The new legislation will enter into force on 1 September 2023. The new framework provides for, inter alia, increased transparency requirements while building on previous concepts of the Swiss data protection regime. In contrast to Regulation (EU) 2016/679 (the General Data Protection Regulation, or GDPR), the FDPA is based on the principle of permitted data processing with exceptions requiring justification (ie, consent, overriding interests or legal bases).

Human genetic testing

Further reforms affecting digital healthcare technologies include a revised regime on human genetic testing. The revised Law on Human Genetic Testing (GUMG), the Ordinance on Human Genetic Testing (GUMV) and the Ordinance on DNA Profiling in the Civil and Administrative Field (VDZV) entered into force on 1 December 2022. Depending on the genetic traits examined, genetic tests are regulated to different degrees. The strictest requirements apply to the use of genetic testing for DNA profiling and in the medical field.

No Swiss artificial intelligence law

Over the past three years, the Swiss government has responded to the increasing importance of AI, answered several parliamentary motions on the subject, published guidelines on risks and opportunities and convened expert panels, including the "Artificial Intelligence Competence Network". The position has so far been that there is no need for general regulation of AI, as the general legal framework in Switzerland is basically suitable and sufficient at the present time.

Switzerland is participating in the negotiations for an international convention on artificial intelligence (AI) as a member of the European Committee on AI (CAI), which was set up by the Council of Europe in 2022.

Swiss providers that place AI systems on the market or put them into operation in the EU are also covered by the territorial scope of the EU AI Act. Under the proposed AI Act, medical devices or in vitro diagnostic medical devices that are themselves an AI system or use an AI system as a safety component are covered by the MDR/IVDR and the AI Act. Furthermore, the AI Act applies to Swiss providers and users of AI systems if the result produced by the AI system is used in the EU. The so-called Brussels effect is likely to occur. Many Swiss AI providers will develop their products not just for Switzerland; meaning that the new EU standards of the AI Act should also become established in Switzerland.

Swiss health data space

On 4 May 2022, one day after the EU Commission had announced its plans for the European Health Data Space, the Federal Council informed the public that it wanted to enable better use of health data for research.

The planned health data space for Switzerland is only intended to serve research. This is in contrast to the European Health Data Space, which gives priority to promoting the empowerment of individuals in dealing with health data.

Currently, the Federal Department of Home Affairs is clarifying the requirements for the proposed system and its legal framework on behalf of the Federal Council.

Reform Impact

Among the regulatory reform projects underway, the new regulations on medical devices and the revised FDPA, as the most far-reaching revisions, are likely to have the greatest impact on

digital healthcare. Their impact is, however, not yet fully discernible, as respective enforcement practices have yet to be adopted.

The further development of the EPD and the plans on a Swiss data space do not seem to be co-ordinated or to follow a coherent strategy. Switzerland still lacks a coherent and efficient environment for the lawful and secure further use of (health) data.

Shifting Practices in Regulatory Oversight

Regulatory oversight has shifted procedurally and substantively – ie, in its focus. Changes are most apparent in digital medicine.

- Procedurally, Swissmedic largely communicates with economic operators via its online portal. Through the portal, it receives market surveillance notifications, applications for authorisations and regulatory documentation, and issues regulatory orders. It is also exploring ways of using machine-learning technologies to search for, analyse and validate scientific evidence or detect patterns or trends in reported adverse events. Swissmedic is in the process of evaluating benefits and risks of using AI technologies for assessing projects for, and the results of, clinical trials. As more scientific disciplines become necessary for an effective oversight, Swissmedic also faces increased complexity in its internal knowledge organisation.
- In terms of regulatory focus, Swissmedic and the FOPH are examining ways to address the trend in precision medicine. Swissmedic also aims at improving transparency on risks relating to digital medicine for patients and users – eg, hacking of insulin pumps or patient records.

2.3 Regulatory Enforcement

Key areas of enforcement are centred around applications causing or contributing to the highest health or privacy risks for patients or users. Thus, enforcement focus lies on high-risk digital medicine applications or other such technologies processing high quantities or a broad spectrum of health-related personal data.

Where authorities open investigations against economic operators, they are generally required to grant those operators a right to be heard, unless the suspected risks require immediate or covert action. Any action would have to be proportionate to the operators' legitimate interests. As a rule, prior to issuing any binding order, authorities will generally have to give addressees of any such order the opportunity to submit a defensive statement. Upon the issuing of a binding regulatory order, addressees have the right to take recourse before an instance specified in the applicable legal regime (eg, the Federal Administrative Court).

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

Certain digital healthcare technologies may be subject to generic, non-healthcare-specific legal regimes, such as telecommunications regulations, general product-safety regimes and competition laws.

Telecommunications Regulations

Digital healthcare technologies qualifying as telecommunications services within the meaning of the Swiss Telecommunications Act (TCA) fall under the Swiss oversight of the Federal Office

of Communications (OfCom) and have certain reporting, co-operation and documentation obligations under the Swiss Federal Act on the Surveillance of Post and Telecommunications (SPTA).

The TCA regulates the transmission of information and is aimed, inter alia, at ensuring cost-efficient, stable, competitive and accessible telecommunications networks in Switzerland. It defines telecommunications services as the transmission of information for third parties. As per guidance provided by OfCom, a telecommunications service provider (TSP) is a person who assumes responsibility for the transmission of end-user signals vis-à-vis end users or other TSPs.

In a decision in April 2021 and along the lines of the European Court of Justice's jurisprudence, the Swiss Federal Court held that an internet-based instant messaging app (such as Threema, Signal or WhatsApp) relying on internet access provided and administered by a third party (so-called over-the-top services, or OTT services) does not classify as a TSP. It follows that to be considered a TSP, digital healthcare technologies would have to exercise some form of control over the transmissions network (eg, through a feed-in interconnection agreement allowing users of an internet-based service to access mobile telephone numbers) or provide a contractual guarantee for the correct and uninterrupted transmission of user information.

OTT services enabling one-way or multi-path communication – eg, offering chat or other communication functions between HCPs and patients – may, however, qualify as providers of derived communication services within the meaning of the SPTA. Such providers of derived communication services face certain, albeit reduced, co-operation and reporting obligations in the surveillance of telecommunications networks.

Product Safety Laws

Digital healthcare technologies may also fall under non-healthcare-specific product safety laws. As a rule, products intended for consumer use are governed by the general requirements on product safety provided by the Swiss Federal Act on Product Safety (PrSG). Regulatory oversight lies with authorities specified in the Swiss Ordinance on Product Safety or other sector-specific ordinances.

By way of an example, wearables measuring vital parameters and wirelessly connected to other devices may need to observe essential health and safety requirements set out by the Swiss Ordinance on Telecommunications Installations. Oversight of the adherence to such essential health and safety requirements lies with the Swiss Federal Inspectorate for Heavy Current Installations.

Competition Laws

Oversight over compliance with the Swiss Cartel Act (CartA) lies with the Swiss Competition Commission. Digital healthcare platforms fostering the exchange of data between competitors (eg, HCOs competing for patients) that has the effect of co-ordinating competitive behaviour (such as setting prices) may fall within the realm of co-ordinated behaviour prohibited under the CartA. Furthermore, recent developments in the EU have spurred debates on whether violations of data protection laws may constitute an abuse of market power under the CartA. Depending on their specific functions, digital healthcare platforms may thus need to take competition laws into consideration.

Data Protection

The Federal Data Protection and Information Commissioner (FDPIC) is appointed to supervise federal bodies, advise private operators and enforce federal data protection law.

Cantonal "public bodies" are subject to cantonal data protection laws and an oversight by the cantonal data protection bodies. A vast number of HCOs qualify as "public bodies".

As the healthcare sector becomes increasingly digital and data-driven, the role of the data protection authorities becomes increasingly important, even though their reach, resources and resolve are not on a par with their European counterparts. Interaction or co-operation by the Swiss data protection authorities with other agencies is subject to alignment in each case and the delineation of authority is often blurry. For example, (only) some cantonal regulators have published extensive guidelines on the use of cloud services by "public bodies".

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

The Swiss healthcare system is based on three pillars of medical care: treatment, rehabilitation and care. Prevention and health promotion are less firmly anchored in the Swiss health system.

The FOPH defines "prevention" as an umbrella term for all measures that are intended to prevent the occurrence, spread or negative effects of health disorders, diseases or accidents. In the field of prevention, a distinction can be made between the following forms of prevention, depending on the timing of the measures:

- primary prevention aims to prevent diseases as far as possible;
- secondary prevention serves to detect diseases at an early stage; and
- tertiary prevention aims to mitigate the consequences of a disease.

A difference between the regulation of preventative and diagnostic medicine arises from the remuneration by the mandatory health insurance. In the case of diagnostic treatment, it is assumed that these medical services comply with the principle of effectiveness, expediency and economic efficiency, which are remuneration conditions. This does not apply to preventative medical services, and all such services are to be paid for by the mandatory health insurance only if specifically included in a list.

4.2 Increased Preventative Healthcare

A quarter of the Swiss population suffers from a non-communicable disease (NCD) such as cancer or diabetes. A healthy lifestyle and knowledge can reduce such diseases or ensure they do not occur. Therefore, care providers such as hospitals and independent health specialists increasingly involve preventative measures in their work for guiding ill people or those at higher risk of disease on how to improve health.

Certain measures of medical prevention are covered by the mandatory health insurance. The costs are paid by the health insurance for prophylactic vaccinations, examinations of the general state of health or the prevention of diseases, among other things.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Lifestyle/Wellness Apps as Medical Device Software

The Swiss Competence and Co-ordination Centre of the Confederation and the Cantons (eHealth Suisse) published the "Guide for App Developers, Manufacturers and Distributors" together with accompanying "Checklists" in April 2022 to help distinguish between "lifestyle/wellness" (sic) products and medical devices. An app only measuring fitness or nutrition data or statistically evaluating clinical or epidemiological data does not qualify as a medical device (see **6. Software as a Medical Device**).

Data Protection

Personal health information, directly or indirectly allowing for insights into an identified or identifiable person's physical or mental health, is categorised as particularly sensitive data under the general data protection regime (see **10. Data Use and Data Sharing**).

Professional and Official Secrecy

HCPs and HCOs are subject to professional and/or official secrecy obligations. Disclosure of secrets (including personal health information of patients) to third parties is prohibited. It is only permissible if mandated or permitted on legal grounds or upon informed patient consent. In contrast, disclosure to auxiliary persons is permitted. IT service providers involved as auxiliaries (subordination) must maintain professional secrecy (see **10. Data Use and Data Sharing**).

4.4 Regulatory Developments

Prevention today is mostly a task for healthcare professionals and non-governmental organisations, such as organisations for the elderly and for cancer patients. Health insurance providers offer services aimed at prevention, but it is not a key task for mandatory health insurance providers, as noted previously. However, the National Strategy for the Prevention of Non-Communal Diseases (NCD Strategy) 2017–2024 aims to strengthen health promotion and increase disease prevention.

4.5 Challenges Created by the Role of Non-healthcare Companies

As there is no uniform legislation in the field of digital health, companies must comply with different laws and regulations depending on the sector affected by the new technology. While healthcare companies are used to the strict sectoral regulation in the healthcare sector and require their contract partners to comply with those regulations, non-healthcare companies are used to more liberal regulations. Therefore, it is particularly important for such companies to contractually agree on the clear distribution of regulatory responsibilities.

If medical advice is provided in individual cases – for example, in the context of telemedicine – this constitutes the exercise of a medical profession and is only permitted for persons with a professional licence.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

Switzerland's digitalisation is progressing more slowly than in other countries. Governmental digitalisation efforts in the health sector have so far focused on the EPD and the necessary interoperability.

This brings into contrast Switzerland's lively start-up scene in the field of digital health. As of mid-May 2023, the "Swiss Healthcare Startups" association alone had 624 start-up members. A majority of them are active in the medtech sector. Wearables, implantables and digestibles are part of the innovation palette that arises from this.

5.2 Legal Implications

Under Swiss law, there are no specific liability rules regarding digital health. In general, civil liability rules apply, especially tortious liability, contractual liability and product liability. Product safety law, which also covers digital health products, establishes strict liability. The manufacturer of products is therefore liable for death, personal injury and property damage resulting from the defectiveness of a product. A manufacturer within the meaning of the Product Safety Act is also anyone who claims to be a manufacturer or whose name or trade mark is affixed to a product. Those who import a product for the purpose of resale, rental or other commercial purposes also qualify as manufacturers.

Concerning the use of AI in healthcare, the liability of physicians must be assessed with regard to a possible breach of the physician's duty of care.

The attribution of liability between the various parties (especially manufacturers, healthcare institutions and healthcare professionals) must be contractually agreed upon.

5.3 Cybersecurity and Data Protection

Health data is considered sensitive personal data under data protection law.

Moreover, when people record data about themselves via fitness apps or wearables, they accumulate large amounts of data. There is a risk of loss of control, which increases the risks from a data breach. If third parties obtain information about health, the data subjects may suffer serious disadvantage.

Inherent in the use of data processing, including of AI, is the risk of unauthorised disclosure of personal data; in the case of AI, this may occur both during the training and the application phase. Added to this risk is the risk of manipulation of training data. Under the FDPA, any personal data must be protected against unauthorised processing through adequate technical and organisational measures, even though the law does not specifically require certain types of measures.

Cybersecurity risks in cloud computing are mitigated to an extent, though legal risks increase, in view of cross-border data transfers and the required transfer impact assessments.

To address these risks, contracts will usually require adequate security measures, and before data is shared with others, a vendor assessment is necessary or, at least, good practice. In addition, contracts will require breach notification, even though under the current FDPA there is no mandatory obligation to notify breaches to the FDPIC, and an obligation to communicate breaches to the data subjects only arises in exceptional circumstances. The revised FDPA (as of 1 September 2023) will introduce mandatory breach notification, largely in alignment with the GDPR.

5.4 Proposed Regulatory Developments

While the TPA provides the general legal framework regarding the manufacture, distribution and use of all medical devices, the MedDO contains a definition of medical devices. Other relevant laws include the FDPA, the FSA and the PrSG.

In addition, legislation on intellectual property and the Federal Act on Unfair Competition can be relevant.

The regulatory authorities in digitalised medicine are Swissmedic, the FOPH and the FDPIC. Swissmedic is responsible for the authorisation and supervision of clinical trials with medical devices and for market surveillance, and the FOPH regulates the reimbursement of costs in relation to medical devices by the OKP. The FDPIC is the supervisory body for compliance with data protection legislation (see **2.1 Healthcare Regulatory Agencies**).

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Definition of Medical Devices Under the MedDO

Based on the principle of harmonisation with EU medical device law, the current Swiss definition of medical devices mirrors the MDR.

In summary, and in line with the EU regulatory framework, a product, including software, is considered a medical device if it is intended by the manufacturer, inter alia, for the (medical) purpose of:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of a human disease, injury or disability;
- investigation, replacement or modification of the anatomy, or of a physiological or pathological process or state;
- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations; or
- controlling conception or making diagnoses in relation to conception (abbreviated definition).

Whether a product is intended for a medical purpose is determined in accordance with the manufacturer's design and claims, as expressed in the product's labelling, instructions for use, documentation and marketing materials. The qualification of a medical device is determined by a subjective-objective test, meaning that arbitrary disclaimers provided by the manufacturer will be deemed ineffective if they are inconsistent with the product's intended functions and objective presentation.

Medical Device Software

On 26 May 2021, Swissmedic issued a guidance document on standalone medical device software, including apps installed on wearable devices, and described practical examples of non-medical software ("Information Sheet on Medical Device Software"). Swissmedic prominently references the MDR guidance MDCG 2019-11, issued by the EU Medical Device Coordination Group (MDCG).

Software performing a certain degree of data processing tailored to individual patients with a view to achieving a medical purpose qualifies as a medical device. As a rule, the following functions do not qualify as medical in nature:

- storage and archiving;
- communication (flow of information from a source to a recipient);
- simple search; and
- lossless compression (ie, compression permits the exact reconstruction of the original data).

There are numerous software applications in the healthcare sector that are not medical devices. General software that does not go beyond imparting knowledge, such as a (non-personalised) information platform or electronic patient dossier, is not considered a medical device. An app only measuring fitness or nutrition data or statistically evaluating clinical or epidemiological data does not qualify as a medical device.

In contrast, an app that measures a woman's fertility by analysing personal data was qualified as a medical device by the Federal Administrative Court.

Software not intended to achieve a medical purpose on its own is not itself considered a medical device, but may fall within the scope of the medical device regime as an accessory to, or component of, a medical device (for example, if it drives or influences a medical device).

Apps recording or using the data of a specific person, though mainly to consolidate and summarise data, can be classified as non-regulated apps in the health sector. Such digital health products can then, despite not being subject to the TPA and the MedDO, be qualified as utility articles that must comply with the provisions of the Federal Act on Foodstuffs and Consumer Products (FSA).

Self-Regulatory Concept of the Medical Device Regime

As in the EU framework, the Swiss ordinances are characterised by a self-regulatory concept based on harmonised technical standards developed by industry organisations and endorsed by Swissmedic. Medical devices do not require a marketing authorisation. To be marketable, they must be marked with a specified conformity marking, which may only be affixed following a specified risk-based conformity assessment. Depending on the medical device's risk profile and corresponding classification, manufacturers must involve third parties in the conformity assessment of their devices – ie, notified bodies accredited by the competent accreditation organisation. Irrespective of their class, all devices must undergo a clinical evaluation procedure based on clinical evidence representative of their risk.

Machine Learning-Enabled Medical Device Software

Medical-device technologies based on adaptive machine-learning algorithms have been described as "black box medicine" due to their evolving "learning" output and opacity. Indeed, machine-learning algorithms are characterised by a certain lack of input-to-output traceability, a fact that poses a hurdle in clinical evaluation. Unlike other regulatory authorities in Europe, Swiss authorities have not yet issued guidance on evidentiary requirements for medical devices based on machine-learning technologies. Respective guidance will likely correspond to guidelines under the MDR and IVDR currently pending with the MDCG. Harmonised technical standards for the general safety and performance requirements specific to machine-learning algorithms have also not yet been endorsed by the Swiss regulators (see **2.2 Recent Regulatory Developments**).

New Market Entries

Software providers that offer software, or parts of a greater system, that qualifies as a medical device are not always mindful at the early stages of planning and development that many applications are caught by the regulatory regime. This tends to delay product development and increases costs. At the same time, the new medical device regime tightens requirements on

documentation, security, connectivity and maintenance, which not all newcomers are prepared to satisfy.

Maintenance (Updates)

According to the TPA, users of the medical device software have a duty to maintain the performance and safety of the medical device. They must follow the manufacturer's instructions for use for the maintenance of the device. The MedDo defines maintenance as "measures such as preventative maintenance, software updates, inspection, repair, preparation for first use and reprocessing for re-use or measures to keep a device in functional condition or restore it to functional condition". The maintenance must be carried out in accordance with the principles of a quality management system (QMS) and must be organised and documented appropriately.

On 12 May 2023, Swissmedic published its report on hospital inspections 2021/2022 and included a strong criticism therein. The maintenance by third parties (most smaller hospitals outsource their maintenance to external service providers) was the aspect most frequently criticised, namely in 84% of the inspections. In 42% of cases, the hospitals did not have an updated equipment inventory or overview of the status of planned maintenance operations by the third-party companies. In 58% of the inspected hospitals, the various maintenance processes and associated interfaces were poorly regulated and documented, and did not satisfy the requirements of an appropriate QMS. The systematic measurement, periodic reporting and continuous improvement of the quality of the internally provided maintenance operations using defined quality indicators were found to be lacking in 42% of the inspections.

It seems reasonable to assume that the maintenance of medical devices by outpatient care providers does not receive great attention.

7. Telehealth

7.1 Role of Telehealth in Healthcare

During the COVID-19 pandemic, the number of long-distance consultations increased sharply in all medical specialties. These were carried out via telephone or simple videoconferencing services. However, the pandemic did not result in the establishment of remote consultations; outside the "gatekeeper" basic insurance model, these have not been widespread. Besides the lack of tariffs, safety and liability concerns are often seen as inhibiting factors.

Apart from a few provisions in cantonal law and an accordingly varying degree of liberality towards telemedicine across the Swiss cantons, there is no telemedicine-specific legislation; telemedicine is thus subject to general rules governing conventional forms of healthcare.

Medical professional standards of care apply. According to the current code of professional practice of the Swiss Medical Professional Association (FMH), telemedical care conforms to professional standards, provided that, as a rule, treatment is not exclusively based on electronic communication or other forms of remote communication.

The current legal issues revolve around the cross-border provision of care and operating licence requirements for telemedical platforms employing or co-operating with physicians.

While the cross-cantonal provision of telemedicine is practically undisputed, licensing require-

ments for physicians and telemedical platforms providing remote services from EU/European Free Trade Association member states are subject to ongoing debate.

In principle, physicians based in the EU/EEA benefit from an exemption from cantonal professional operating licensing requirements. However, there is currently no jurisprudence or consensus in doctrine on whether telemedical services provided from EU/EEA states without cantonal licences would be subject to the limitation of 90 days per year provided for cross-border services based on the sectoral agreements between the EU and Switzerland. Arguably, the limitation only applies to a physical presence in Switzerland and does not extend to remote telemedical services. Nevertheless, the EU's notation of services also encompasses correspondence services, suggesting an according interpretation of the term under the sectoral agreements.

Similarly, jurisprudence has not yet been rendered on the question of whether, and to what extent, a physician's medical practice will be governed by foreign or Swiss professional standards (country of origin versus country of destination principle). Much like in the EU, an established practice and jurisprudence is lacking. Since Switzerland is not bound by the EU's patchwork of directives touching upon cross-border medical professional services, the Swiss regulators are not bound by an interpretation of these directives adopted under EU law.

In recent years, certain cantonal authorities have argued that telemedical platforms acting as intermediaries between physicians and patients would require cantonal operating licences and an establishment in Switzerland. Telemedical platforms thus have to consider whether they are defined as outpatient medical institutions within the meaning of health insurance law licensing provisions. If this is the case, they will only be admitted to providing services under the mandatory health insurance scheme if all their physicians would also (as individual physicians) meet the admission requirements. This can be a real stumbling stone. Physicians are required to have had three years of training at a Swiss continuing education institution (with exceptions) as well as proficiency in the official language of the canton that issued the operating licence for the institution (subject to a purpose-based interpretation, the destination of the remote counselling does not matter).

7.2 Regulatory Environment

During the COVID-19 pandemic, the medical professional association FMH partnered with a videoconferencing service, offering physicians its platform free of charge. Guidance issued by the FMH during the pandemic specifies that the responsibility for the use of messenger or video services lies with the respective physician. To aid decision-making in the choice of a service, the FMH published guidance listing the most common products for video consultations, including a risk assessment available on its website.

7.3 Payment and Reimbursement

The tariff structures for outpatient treatments are negotiated between tariff partners specified in the health insurance statutes – ie, representatives of health insurers and professional associations.

The applicable tariff (TARMED) currently lists only one position, "Telephone consultation by the specialist". However, this tariff item is strictly limited. As a rule, 20 minutes per session can be billed. For psychiatrists, there are separate specific tariff positions, which are also limited. During the COVID-19 pandemic, the respective

tariff positions were partially and temporarily adapted to account for the need for longer teleconsultations.

The outpatient tariff is to be modernised after almost 20 years; related negotiations are ongoing.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

The term "internet of medical things" (IoMT) refers to wirelessly connected sensors transmitting information to other objects in the healthcare ecosystem by way of machine-to-machine communication. Possible applications include inventory or occupancy management in HCOs or real-time monitoring of vital signs in patients.

A systematic roll-out of IoMT applications in healthcare will trigger and amplify general legal issues, including those previously mentioned, such as data privacy and data security, and will expose HCOs, HCPs and patients to new security risks such as hacking, hijacking and manipulation of digital assistants ("vulnerability by design" due to different, often low safety levels). Such risks may raise questions as to whether Swiss regulatory regimes address those risks sufficiently and whether the current criminal provisions are effective in combating related crimes.

The Swiss Federal Council (FC) published a report dated 29 April 2020 on security standards for internet of things devices that found that fragmented regulations across domestic jurisdictions may prove ineffective and lead to unintended market distortions. International coordination will be necessary.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

With transmission speeds approximately 100 times faster than 4G networks, the implementation of 5G may further accelerate the development of digital healthcare.

In telehealth, 5G has the potential to unlock the use of virtual reality technology or sensors to enable treating physicians to monitor a patient's vital parameters. One possibility further attributed to 5G is providing grounds for virtual computerised replication of a surgical procedure remotely controlled by a physician at the patient's site (as part of a vision termed the "tactile internet"). To achieve 5G's potential in remote surgical interventions, telecommunications providers will have to ensure very low latency and transmission priority in their networks, and healthcare providers will need to take care when drafting appropriate contractual provisions to address liability risks.

5G may also underpin treatment in disaster areas by enabling real-time tracing of large populations or facilitating inventory and supply management within HCOs.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

Using and sharing personal health information within the scope of the Swiss jurisdiction may be subject to parallel legal regimes, including:

- general data protection law;
- (medical) and/or (official) secrecy rules; and

• human research regulations.

General Data Protection Laws

Personal health information (PHI), directly or indirectly allowing for insights into an identified or identifiable person's physical or mental health, is categorised as particularly sensitive data under the general data protection regime (revision discussed under **2.2 Recent Regulatory Developments**).

Under the revised FDPA, processing PHI in breach of general principles on transparency, good faith, proportionality, data accuracy or data security, as well as transferring PHI to other controllers, requires a justification. Such justification may lie in:

• a legal basis allowing for such a transfer;
• data subject consent; or
• an overriding private or public interest.

As a rule, a justification is not necessary where a recipient acts as a processor on behalf of a controller and is subject to respective auditing and instruction rights.

Where consent is required for lack of other justification, it must be informed, voluntary and explicit. In principle, consent may be provided in any form, including orally or electronically. Where processing activities and purposes are not self-evident and reasonably transparent from the circumstances, consent must be based on adequate information detailing the respective processing purposes.

It is often difficult for healthcare customers to assess whether suppliers of emerging technologies are providing adequate cybersecurity – ie, using state-of-the-art technologies. Unsurprisingly, HCPs and HCOs often cite concerns about not meeting data protection and data security requirements as a reason for their reluctance to use today's digital opportunities.

PHI may be transferred abroad under the conditions set out in the FDPA. The USA, for example, does not provide an adequate data protection level within the meaning of the FDPA. In 2020, the Swiss FDPIC published a position paper concluding that a certification under the Swiss-US Privacy Shield no longer constitutes a sufficient basis for personal data transfers to the USA. An adequate data protection level must therefore be ensured by other means. In practice, this is achieved contractually, by concluding a data transfer agreement, typically using EU standard contractual clauses adapted to Swiss requirements with additional safeguards depending on a case-by-case analysis.

Anonymised and Encrypted (Including Pseudonymised) PHI

In principle, Swiss data privacy laws do not apply to anonymised data or object data unrelated to an identified or identifiable person. Like the GDPR, Swiss law is based on a relative qualification, meaning that data will be qualified as "personal" depending on whether the controller, processor or recipient of the data can relate that data to an identified or identifiable person using reasonable means. Conversely, data is considered anonymised where identification is practically impossible because it requires efforts prohibited by law or reasonably disproportionate to any interest in that identification, such that the person in possession of the data would not be expected to take any such means.

Where merging of multiple data sources leads to, or allows for, an identification of data subjects, the resulting personal data is subject to the data protection regime.

Data encrypted according to the current encryption standard, decipherable only to the person in possession of the relevant key, does not qualify as personal data regarding processing activities carried out on that encrypted data by a third party. To fall outside the scope of the general data protection provisions, the controller must ensure that only authorised persons have access to the decryption key and that data cannot be decrypted without the decryption key.

Professional and Official Secrecy

HCPs and HCOs are subject to professional and/or official secrecy obligations.

- The federal medical secrecy (Swiss Criminal Code, CC) applies to doctors, dentists, chiropractors, pharmacists, midwives, psychologists and the auxiliary of any of these persons. Auxiliary persons include, for example, nurses, medical practice assistants and occupational and physical therapists. In the case of other professional groups that also process health data, cantonal statutory confidentiality obligations may apply.
- Members of an authority and/or public officials and the auxiliary of any of these persons have an official secrecy obligation (CC). This covers both institutional and functional (ie, performance of public duties) public officials. Official secrecy obligations may apply – eg, in the case of health data processed by employees of a public hospital.

Disclosure of secrets (including PHI) to third parties is prohibited. It is only permissible if mandated or permitted on legal grounds (eg, written authorisation of the superior authority) or upon informed patient consent. Consent may be express, silent or by implied conduct. Implied conduct plays an important role in practice.

In contrast, disclosure to auxiliary persons within the meaning of these provisions is permitted.

- Doctrine and practice (most recently the FDPIC in particular) refer to IT service providers as auxiliary persons, if they support the physician in the performance of their work. If they can, in principle, access patient data, they must therefore maintain professional secrecy (and must be informed and obliged accordingly).
- The question of whether IT service providers (including foreign providers) can be auxiliary persons under official secrecy was discussed in an expert opinion from 16 September 2021 (on cloud use by the city of Zurich). It was confirmed that outsourcing was not illegal if done correctly. This requires that the IT service provider must be involved as an auxiliary (subordination).

(Human) Research Laws

The data protection provisions (recently revised, see **2.2 Recent Regulatory Developments**) in the Human Research Act (HRA), the Ordinance on Clinical Trials (ClinO) and the Human Research Ordinance (HRO) are lex specialis to general data protection provisions.

In deviation from the general data protection laws, the HRA does not recognise any research privilege that would make consent redundant. As a rule, the consent of the data subject is required. In certain cases, the absence of an objection is sufficient. In both constellations, an approval from the ethics committee is required.

- Biological material and genetic data may be further used for research purposes as follows:
  (a) in unencrypted form if the data subject gave informed consent (consent cov-

ers further use for one specific research project);
(b) in encrypted (pseudonymised) form if the data subject gave informed consent (consent covers further use for research projects in general); and
(c) in anonymised form (the absence of an objection after sufficient information allows for anonymisation).

- Non-genetic health-related data may be further used for research purposes as follows:
(a) in unencrypted form if the data subject gave informed consent (consent covers further use for research projects in general);
(b) in encrypted (pseudonymised) form in the absence of an objection after sufficient information (absence of objection covers further use for research projects in general); and
(c) in anonymised form (not regulated in the HRA).

Foreign data transfers of genetic research data are only permissible if they are carried out for research purposes and the data subject gave their informed consent. Non-genetic research PHI may be transferred abroad under the conditions provided in the FDPA.

Liability Risks

Violations may result in sanctions for the company as well as fines (up to CHF250,000) for natural persons. The authorities may conduct investigations or issue orders to restrict, modify or stop processing. The disclosure of data within the scope of professional confidentiality may result in additional sanctions. Only some intentional violations are punishable (eg, failure to inform about the processing, or use of a processor without proper appointment). Violations can also lead to civil liability (claims for damages).

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

While the systematic use of technologies based on intelligent (learning) algorithms is still largely experimental in digital therapeutics, machine-learning technologies are gaining ground in, for example, diagnostics, the discovery of new medicinal product candidates or pattern recognition of trends in side effects.

With many applications still at an experimental level, the Swiss regulatory regime has not kept pace with their growing potential. AI-specific Swiss regulations have not yet been adopted. As with medical device software (see **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies**), guidance on evidentiary requirements for general healthcare applications has not yet been set. AI-enabled and machine learning-enabled technologies are thus subject to general principles applicable to the respective product category.

Hence, the use of real-time or real-world data as training data and the according risk of perpetuating system bias is currently not specifically addressed under Swiss law, nor have data access regimes been specifically adapted to the machine-learning context and to the fact that machine-learning algorithms require significant amounts and ranges of training data to reach their full potential. The Swiss EPD is based on patient consent and is not designed to enable insights based on linking patient records.

11.2 AI and Machine Learning Data Under Privacy Regulations

The European Commission's proposed regulation on AI mainly regulates high-risk AI applications, including the use of AI in medicine. Such

applications will need to meet transparency requirements, among other requirements.

In Switzerland, general regulation of AI has so far been rejected, and no specific regulation is foreseeable, except that the FC adopted guidelines for handling AI by the federal administration in 2020. On 13 April 2022, the Federal Council took note of the report "Artificial Intelligence and International Rules" by the Federal Department of Foreign Affairs (FDFA). The report sets out various measures for allowing Switzerland to play an active role in shaping and contributing to an appropriate global set of AI rules.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Where AI or machine-learning devices or software are designed to serve a medical purpose directed at an individual person, these devices may qualify as medical devices under the MedDO. When qualifying an e-health product as a medical device, the regulations on the conformity of medical devices must be observed. There are different approval and authorisation requirements, depending on the classification of a medical device. Each medical device must be assigned to a class before being placed on the market in Switzerland. Based on the intended purpose and depending on the risk potential of a medical device, classification can be made in Classes I, IIa, IIb and III. The revision of medical device law has led to a higher classification of mobile applications and thus to stricter regulation. Health apps are now regularly assigned to Class IIa. Medical devices that are assigned to Class IIa must, in particular, be assessed by an accredited conformity assessment body. In this regard, a risk assessment shall be carried out, determining the safety of the respective device.

In addition, developers must be mindful of increased expectations for security and data protection of customers and stakeholders and apply high standards in this regard.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

To support digital healthcare, HCOs need an adequate IT infrastructure suitable for integrating new technologies. Key features of digital healthcare build on connectivity between interoperable technologies. To ensure interoperability, the infrastructure must be based on common standards. These standards are still under development. In addition, secure and effective sharing of information relies on stable networks equipped with sufficient capacity. As with all systems enabling multiparty co-operation, security issues become particularly important, as does data and information governance.

13.2 Data Management and Regulatory Impact

Although the FDPA calls for data security measures that correspond to the state of the art, it does not specify the precise technical standards in more detail. The FDPO contains more detailed regulation, but no specific requirements for IT upgrades. Generally, similar requirements as for new software will apply, including privacy-by-design and privacy-by-default requirements.

14. Intellectual Property

14.1 Scope of Protection

Under Swiss law, computer programs may be protected by non-registrable copyrights. Unlike in other jurisdictions, commercial intellectual property rights to such computer programs are freely assignable. According to the currently prevailing opinion in doctrine, associated moral rights, such as the right to be named as an author, are non-transferrable, but may be waived. Arguably, their exercise may also be delegated to third parties.

Software as such is not patentable. However, inventions may be patentable provided they have a technical implementation.

The question of how inventions and works of authorship created by AI-based technologies are allocated has not yet been decided. Like the European Patent Office, the majority in doctrine argues that inventorship in patent law – and authorship in copyright law – can only be attributed to natural persons.

14.2 Advantages and Disadvantages of Protections

Patents provide an exclusive right to use the invention commercially, including manufacturing, marketing, importing and exporting. However, private use, research and teaching remain permitted for anyone.

Literary and artistic intellectual creations of an individual character, including computer programs, are subject to copyright protection, regardless of their value or purpose. Such creations are automatically protected. The author has an exclusive right in their own work and the right to recognition of their authorship.

Trade mark and design legislation protects branding but not, generally, the function of products or services.

Switzerland does not have any specific trade secret laws except provisions in criminal and unfair competition law and obligations of secrecy in certain types of contracts. Not being an EEA member state, Switzerland has not implemented the EU Trade Secrets Directive.

14.3 Licensing Structures

There are no formal requirements regarding the licensing of IP rights under Swiss law. Nevertheless, it is customary and advisable to enter into a written licence agreement and to register the licence (otherwise a licensee cannot enforce its licence rights against a third party who acquires the intellectual property rights in question in good faith).

14.4 Research in Academic Institutions

Under Swiss general contract laws, designs and inventions conceived or reduced to practice in the performance of an employment agreement belong to the employer. A similar provision is stipulated for computer programs protected by copyrights under the Copyright Act. According to this provision, the employer shall have exclusive rights of use in a computer program created by its employee in the course of the performance of the employee's contractual obligations.

Where private sector technology companies are involved in developing a device or medical innovation, intellectual property rights are often allocated to the private sector company funding the research. In practice, research institutions often reserve the right to use intellectual property developed during the collaboration for non-commercial purposes. In some cases, such

a reservation may be mandated under competition law considerations.

Competition law considerations also play an important role in licensing agreements. For example, contractual clauses creating an obligation on the licensee to assign or grant an exclusive licence to a licensor (or a third party designated by the licensor) for any improvements made on the licensed technology require careful assessment.

14.5 Contracts and Collaborative Developments

Given the strictures imposed by intellectual property statutes for multiparty inventions and works of authorship, contractual arrangements often regulate cross-licences in background intellectual property rights, and the allocation of (joint or separate) ownership in foreground intellectual property. Best practice includes fine-tuning the allocation of intellectual property rights to the specific needs of the parties and an awareness that intellectual property allocation is not an issue that should be left to lawyers, but requires business buy-in and alignment with the broader strategies of the parties.

15. Liability

15.1 Patient Care

General Principles of Liability

Liability for patient care can be based on:

- the Swiss Product Liability Act (PLA), establishing strict liability for defective products modelled after the EU's Product Liability Directive 85/374/EEC (PLD);
- contractual provisions governed by the Swiss Code of Obligations (CO); or
- the CO's general regime on torts.

In contrast to the PLA, liability under the CO generally requires negligence, with the onus of proof lying on the claimant or the defendant, depending, in principle, on whether damages are sought under contract or tort. While strict liability under the PLA cannot be excluded, liability under the CO can be limited to gross negligence and intentional misconduct.

Liability for AI-Enabled Products

As part of an assessment on the need for regulatory reform tailored to AI technologies, the FC entrusted a working group under the auspices of the Swiss Federal Department of Economics, Education and Research with analysing the Swiss regulatory landscape. In its report, the working group held that the current Swiss liability legislation is broad enough to accommodate liability risks emanating from AI. Following the report, the FC concluded that new regulations addressing liability for AI are currently not a priority.

However, spurred by a project to revise the EU's PLD, multiple scholars in doctrine have recently argued for a revision of the Swiss PLA. Referencing an ongoing international debate, they identify three risks inherent to AI:

- the risk derived from the fact that, by definition, AI systems exercise a certain degree of autonomy;
- risks related to their interaction with humans training the AI; and
- their interdependence with other systems – eg, healthcare ecosystems.

Arguments for a revision project are centred on:

- the definition of a product defect and causality;

- the allocation of responsibility between manufacturers and users (risk governance); and
- the burden of proof.

Under the present regime, robots are not endowed with a legal personality; liability lies with a natural or legal person responsible for the damages caused by such robots. Whether the responsibility is with the manufacturer marketing a product or the user training a product with user data depends on an allocation of risks between the manufacturer and the user and the definition of a product defect. Much like the EU's PLD, the Swiss PLA defines product defects referencing the legitimate safety expectations of the public. These expectations are shaped by industry standards. Much will thus depend on the development of adequate standards by standardisation committees, such as the International Organization for Standardization and the International Electrotechnical Commission. Where users play an integral role in training an AI post-market, the manufacturer's influence on compliance with such standards is significantly reduced. Two of the suggestions for reform brought forward in doctrine therefore include provisions on strict liability of users training the devices and/or mandatory insurance schemes.

There are no concepts under Swiss law that specifically address AI and potential bias. Generally, the use and outcomes of AI are attributed to the party or parties that make use of AI-enabled systems. With respect to end-user data, the revised Swiss data protection regime (likely entering into force by 1 September 2023) requires the controller(s) to inform users about automated decisions, where these could have a substantial adverse effect on end users, and allows them to challenge the decision and have it reviewed by a natural person.

15.2 Commercial

Damages for harm incurred by an HCO due to disruptions in the commercial supply chain caused by third-party vendors' products or services will often depend on contractual arrangements between the HCO and the seller or service provider, and on the latter's arrangement with third-party vendors. Should damages from the direct contractual partner of HCOs be unattainable for legal or other reasons, Swiss jurisprudence has established principles regarding:

- third-party liquidation;
- the concept of a contract with a protective effect in favour of third parties;
- enabling liquidation of damages suffered by a non-contracting party; or
- a reversal of the onus of proof under the principle of producer liability in tort.

Whether and which of these principles applies will depend on the specific facts of the case.

Another way in which HCOs may safeguard their interests includes by securing indemnity undertakings from their direct contractual partners.

Trends and Developments

Contributed by:
David Vasella and Anne-Catherine Cardinaux
Walder Wyss Ltd

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today the firm has more than 250 legal experts in six offices in Switzerland's economic centres. It is fully integrated, adapts to clients quickly, and does not hide behind formalism. Walder Wyss Ltd is the first large Swiss firm with a strong focus on tech, including data protection. Its team is familiar with recent developments not only on an academic level but also with hands-on experience from a wide range of projects. Its health sector clients represent all relevant stakeholder groups – pharmaceutical, biotech and medtech companies (including start-ups in early-stage development phases), service providers ranging from individually practising physicians to large hospital and pharmacy groups, clinical research organisations, and health insurers. Its data and technology lawyers share the same team with their healthcare and life sciences colleagues, enabling the firm to quickly navigate the cross-sectional topic of digital healthcare.

Authors

David Vasella is a partner and co-head of Walder Wyss Ltd's regulated markets, competition, tech and IP team. He advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. David deals with cross-jurisdictional data protection projects, including GDPR implementation, data retention, e-discovery, cloud projects, digital marketing, online regulation, information technology and e-business matters. He also regularly advises in relation to commercial IP matters, regulated products and market practices. In addition, he frequently speaks and publishes in his areas of expertise. David is an editor of the Swiss journal for data law and information security, is CIPP/E certified, and is a member of the professional bodies IAPP and DGRI.

Anne-Catherine Cardinaux is an associate in Walder Wyss Ltd's regulated markets, competition, tech and IP team. She advises and represents clients in all areas of constitutional and administrative law and specialises in life sciences and health law. Recently, she advised on the health law requirements for cloud projects and assessed the implications of health apps qualifying as medical devices. Prior to joining Walder Wyss Ltd, she worked as a postgraduate in the legal department at the Basel headquarters of one of the world's largest pharmaceutical companies, as a law clerk at a Zurich district court and as a junior associate in the M&A team of a leading Swiss commercial law firm in Zurich.

Walder Wyss Ltd

Seefeldstrasse 123
PO Box
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss attorneys at law

Introduction

The COVID-19 pandemic highlighted the potential of digital technologies for tackling global health challenges. It also propelled a health technology boom in some countries.

However, digitalisation of healthcare in Switzerland is progressing more slowly than in other countries.

- Although Switzerland has required the introduction of an electronic patient record (EPD) by law since 2017, until recently this only applied to inpatient service providers. For patients, the use of the EPD remains voluntary.
- Remote monitoring of chronically ill patients is mostly limited to pilot programmes, partnerships and research studies by healthcare providers, technology companies and insurers.
- Remote consultations outside the "gatekeeper" basic insurance model have not been widespread.
- There are some partnerships regarding digital therapies. Selected disease-specific apps have been introduced. In addition, a consortium of insurers and providers launched the first digital health platform called "Well" in 2021. Switzerland has yet to include digital therapies in standard care and to support their reimbursement.

eHealth Suisse, which is supported by the federal government and the cantons, refers to a recently published report by the Swiss Health Observatory (OBSAN) on the study entitled "Physicians in Primary Care – Situation in Switzerland and in International Comparison". The report concludes that Switzerland is still lagging far behind in the digital transformation of the healthcare system by international standards. This is particularly noticeable in the eHealth offering for patients and in interprofessional co-ordination.

The slow digitalisation of healthcare stands in contrast to the innovation taking place at a fast pace in the country. Switzerland has a lively start-up scene in the field of digital health. In particular, the École Polytechnique Fédérale de Lausanne (EPFL) and the Swiss Federal Institute of Technology (ETH) in Zurich are innovation drivers. Start-up incubators and government-funded programmes also foster innovation. There is a very active investor scene, consisting of both traditional venture capital and private equity, as well as of large industrial companies.

Causes for slow digitalisation in Switzerland

Some causes are systemic, and solutions cannot be expected overnight. In the context of digital health, there has been no actual political leadership in the past. The Swiss health system has many different actors and responsibilities at all federal levels. This results in a fragmented stakeholder landscape. The legal landscape is characterised by a high degree of complexity, and regulations are implemented through a decentralised approach. This is increasingly evident in health regulations that are not tailored to digital health technologies.

There is also no holistic approach to health data management. Switzerland lacks a coherent and efficient environment for the legitimate and secure re-use of health data.

Recent Regulatory Developments in Terms of Health Data

The COVID-19 pandemic made the health data regulatory deficiency visible in Switzerland. Research, industry and politicians are increasingly commenting on the problem, with "isolated solutions" and "data silos" often being mentioned as keywords.

Since the pandemic, a lot has been happening in terms of health data, secondary use and data spaces. Various reports have been written and projects launched at the federal level. In April 2022, the Federal Council gave information on its plan to develop the EPD further – ie, that it shall become an instrument of mandatory health insurance, and all health professionals working in outpatient care shall be obliged to maintain an EPD. The Federal Council also plans access for research purposes with the consent of the persons concerned.

It should also be possible to use the technical infrastructure of the EPD for additional services. On 4 May 2022, one day after the EU Commission had announced its plans for the European Health Data Space, the Federal Council informed the public that it wanted to enable better use of health data for research.

It seems, however, that the various projects are not especially co-ordinated with each other. A coherent strategy or a comprehensible data and digitalisation policy is not in place.

Among the ongoing reform projects likely to impact the most on innovators in healthcare are the two new medical device ordinances, mirroring the EU MDR and IVDR, and the reformed data privacy regime set out in the Federal Data Protection Act (FDPA) and its implementing ordinance. These two reform projects are dealt with in more detail below.

Reform of the Medical Devices Regime

On 26 May 2021, the revised Medical Devices Ordinance (MedDO) and on 26 May 2022 the new Ordinance on In Vitro Diagnostic Medical Devices (IvDO) entered into force. This revision harmonised the Swiss regime with EU Regulations (EU) 2017/745 (MDR) and (EU) 2017/746 (IVDR).

For the past two decades, Swiss and EU manufacturers of medical devices have benefited from mutual market access thanks to a mutual recognition agreement (MRA) between Switzerland and the EU. Due to the failed negotiations between the EU and Switzerland on the institutional framework agreement, the MRA has been suspended for classical medical devices since 26 May 2021 and for in vitro diagnostic medical devices since 26 March 2022.

As a result, Swiss manufacturers of in vitro diagnostic medical devices are now treated as established in a third country, and must appoint an authorised representative based in the EU and label products accordingly. In addition, the European Commission clarified on 24 May 2022 that Swiss certificates of conformity will not be recognised in the EU, even if the certificate of conformity was issued before 26 May 2022.

This contrasts with the legal regulation of imports into Switzerland, which stipulates that EU certificates of conformity continue to be recognised. In particular, the provisions on the unilateral recognition of EU certificates of conformity are intended to reduce disruptions in the supply of in vitro diagnostic medical devices in Switzerland. Supplementary requirements such as the registration of economic operators and the reporting of serious incidents to the Swiss Federal Agency for Therapeutic Products (Swissmedic), as well as the establishment of a so-called Swiss authorised representative for foreign manufacturers, help to ensure that Swissmedic can maintain market surveillance despite being excluded from the network of EU authorities.

As there is no access to the European database EUDAMED, Swiss economic operators (manufacturers, importers and authorised representatives) must register with Swissmedic. This requirement may lead to EU manufacturers not being prepared to disclose the entire technical documentation to the Swiss authorised representative (especially where importers wish to assume the role of authorised representative for several manufacturers) (business secrets) and therefore preferring not to place the product on the Swiss market. To counteract a possible supply gap in Switzerland in such a case, as an alternative to keeping a copy of the technical documentation available at the authorised representative's premises, the foreign manufacturer is also permitted to send the data directly to Swissmedic.

In terms of digital healthcare, the medical device reform will affect software with an intended medical purpose defined in the MedDO, as well as software driving or influencing a medical device. By contrast, digital healthcare technologies providing, for example, generic non-tailored health or nutrition information, or mobile applications processing sensor data solely for fitness or wellness purposes, would fall outside the MedDO's scope. To guide app developers and help them navigate regulatory qualification, the Swiss regulators have endorsed recommendations and a catalogue of quality criteria for mHealth applications.

Revised Data Protection Act

In view of adapting the Swiss data protection regime to the digital age and to account for the pivotal role of personal data, the Swiss legislature has enacted a revised FDPA, which will come into force on 1 September 2023. The FDPA is largely aligned with Regulation (EU) 2016/679 (the General Data Protection Regulation, or GDPR), but with some significant deviations. The FDPA will be accompanied by a revised ordinance to the FDPA (FDPO). Inter alia, the revised regime increases transparency requirements and liability risks for controllers.

As under the GDPR, personal health information (PHI) belongs to a special category of personal data requiring an elevated level of protection and security. While the definition of PHI under the revised FDPA will not change fundamentally, the definition will be supplemented with additional categories of genetic data and biometrical data "uniquely" identifying a natural person.

Inter alia, current debates are centered around foreign transfers of PHI. Following the decision of the European Court of Justice in re Schrems II, the Swiss Federal Data Protection and Information Commissioner (FDPIC) considers that a certification under the Swiss–US Privacy Shield no longer justifies transfers of personal data to the USA under the FDPA. Thus, transfers must be based on other means – eg, data transfer agreements. Most importantly, the revised standard contractual clauses (SCCs) passed by the European Commission on 4 June 2021 have been recognised by the FDPIC. However, according to the FDPIC, the new EU SCCs only allow the transfer of personal data to states without adequate protection "if the necessary adaptations and additions are made for use under Swiss data protection law". From a Swiss perspective, exporters would therefore have to slightly amend the respective SCCs (with Swiss additions). In addition, data transfer agreements must be accompanied by a transfer impact assessment and potentially by supplementary technical or organisational measures.

Switzerland is regarded as a "third country" from the EU's perspective. However, the European Commission decided on 26 July 2000 that Swiss law provides adequate protection of personal data, and therefore that data transfers from member states to Switzerland are, in principle, permitted. Switzerland's level of data protection is now subject to review for the first time in two decades, and for the first time under the GDPR. A new adequacy decision was originally expected by 2020. However, the decision was postponed, and the EU decision on the continued recognition of the adequacy of Swiss data protection legislation is still pending.

Regulatory Aspects on the Horizon

Regulatory aspects on the horizon include questions on:

- the cross-border provision of medical care;
- product liability and evidentiary requirements for machine learning-enabled devices;
- data access rights unlocking research and innovation;
- interoperability standards; and
- reimbursement of new technologies under the mandatory statutory health insurance scheme.

The soon-expected introduction of the tariff for outpatient services will be of great importance. It has been modernised after 20 years and should better reflect technical developments.

As a market intertwined with the EU, Switzerland follows developments in the EU's regulatory landscape closely, while generally keeping a pragmatic and liberal approach to regulation. In Switzerland, the position has so far been that there is no need for general regulation of AI, as the current general legal framework in Switzerland is basically suitable and sufficient. In particular, the view is expressed that no general AI law should be created, but that sector-specific and technology-neutral regulation should be examined in Switzerland. Moreover, with data protection, Switzerland already has a regulation that covers AI. In particular, the revised FDPA stipulates that data subjects have a right not to be judged by an AI when making important value decisions.

USA

Law and Practice

Contributed by:
Nadia de la Houssaye, Allison Bell, Keiana Palmer and Chino Onubogu
Jones Walker LLP

Contents

Jones Walker LLP is among the largest law firms in the United States, with more than 350 attorneys across the Southeast and other strategic locations, including Miami, New York City and Washington, DC. Led by a core group of veteran healthcare attorneys, the firm's healthcare industry team includes attorneys from all of the firm's major practice areas, who all have extensive experience in specific practice areas, as well as in-depth knowledge of today's healthcare marketplace and regulatory environment. Jones Walker's nationally recognised digital health and telemedicine team has been actively assisting healthcare entities with the structuring and integration of telemedicine systems for more than 20 years. These healthcare entities range from large hospital systems that cross state borders to hospital-based physician practices, direct-to-consumer telemedicine providers, and manufacturers of medical devices used in telemedicine monitoring and diagnoses.

Authors

Nadia de la Houssaye is a partner in Jones Walker' litigation practice and co-leader of the healthcare industry team. She works extensively with hospitals, health systems, providers and start-up companies to structure and integrate telemedicine, telehealth and digital health platforms. Her passion for the expansion and growth of telemedicine began in 1997, when she co-created and helped launch one of Louisiana's first teleradiology networks. Since 2004, Nadia has provided strategic counsel to healthcare providers and hospital systems on telemedicine service lines, including international telemedicine arrangements involving multistate and international licensure and scope of practice issues, cross-border compliance issues, patient consent requirements, commercial payor reimbursement issues, Medicare and state Medicaid billing requirements, and coverage and reimbursement issues.

Allison Bell is a partner in the Jones Walker corporate practice group, and co-leader of the healthcare industry team. She has extensive experience in advising public and private healthcare providers and companies in acquisition and divestiture transactions, mergers, joint ventures and other complex business transactions. Allison also represents not-for-profit and for-profit healthcare providers in unique healthcare-related transactions, including joint operating agreements and complex strategic affiliations. She currently represents the largest health system in Louisiana.

Keiana Palmer is an associate in Jones Walker's corporate practice group and represents private and public companies, institutional investors and other clients in a wide range of corporate and commercial law matters. She has experience in advising high-growth digital health and technology start-ups on entity formation and conversion, corporate governance, regulatory compliance, risk management and strategic planning, among other matters. She has also represented organisational stakeholders; reviewed, drafted and negotiated a variety of commercial contracts; and assisted a range of clients with corporate transactions.

Chino Onubogu is an associate in the Jones Walker corporate practice group, and provides broad-ranging counsel to clients across the country with interests and operations in diverse industries, including healthcare and technology. Chino has experience in drafting corporate agreements, technology transactions and regulatory opinion letters for digital start-ups and healthcare practices. She has also assisted clients with various corporate matters, including corporate governance, multistate entity formation and licensing, entity conversions, data privacy compliance (HIPAA, federal and state), digital implementation of services, and corporate practice of medicine issues.

Jones Walker LLP

201 St. Charles Ave
New Orleans
LA 70170-5100
USA

Tel: +1 504 582 8000
Fax: +1 504 582 8583
Email: ndelahoussaye@joneswalker.com
Web: www.joneswalker.com

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

In the United States, "digital healthcare" is a broad term that covers a variety of health-related products, tools and services distributed through, or making use of, technological solutions to improve mental and physical health and overall wellbeing. These can range from consumer health and wellness apps that are not regulated by the US Food & Drug Administration (eg, the suite of "Apple Health" apps that are available on devices such as the Apple Watch and iPhone) to digital treatments that are regulated by the Food & Drug Administration (FDA) and meet the agency's definition of "software as a medical device" (SaMD; this could, for example, include computer-aided detection software that processes images to help detect breast cancer) – and a host of products, tools and services in between.

Generally speaking, "digital medicine" and "digital therapeutics" are somewhat interchangeable terms that refer to tools, solutions and processes that actively prevent, diagnose, treat or provide therapeutics to address specific diseases or conditions. As such, digital medicine and digital therapeutics are somewhat narrower categories that fall under the umbrella of digital healthcare.

From the perspective of providers, patients and payers, digital medicine and digital therapeutics typically include products and services such as office visits, remote consultations, prescription drugs, surgical procedures, etc, that require the direct involvement of a provider and a patient (and/or the patient's designated caregivers), most of which can be billed and reimbursed through private or public insurance programmes or paid for out of pocket by the responsible party. Technology solutions such as electronic health records, workflow management, staffing software, decision-support software, etc, that are directed toward operational, disease prevention, community health, infrastructure support, accounting and finance, hospital administration and other areas of modern medical practice – but are not directly related to the treatment of individual conditions – are seen as falling under the digital healthcare framework.

1.2 Regulatory Definition

In the United States there is no single or universal definition of digital health or digital medicine. Despite the generally understood difference between digital health and digital medicine solutions noted in **1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics**, federal and state legislation, the regulations that arise out of such legislation, and the agencies that define and enforce these regulations often provide specific definitions that conform to the specific issues, services, conditions, solutions, tools and technologies that are the focus of that particular piece of legislation.

These laws and regulations cover areas such as:

- the collection, use, management, storage and disposal of protected health information;
- data breach reporting and response;
- biometrics;
- product advertising;
- reimbursement;
- government contracts and procurement;
- genetic testing;
- the full suite of "tele-" services (telemedicine, teledentistry, tele-counselling, etc);
- diagnostics;
- therapeutics;
- online pharmacies; and
- practitioner licensing, etc.

The definitions of digital health and digital medicine provided in one piece of legislation, regulation or other federal and state guidance cannot be assumed to apply, exactly, in legislation regarding other issues.

1.3 New Technologies

Most of the technologies that support advances in digital healthcare are not exclusive to this industry. Mobile devices and networks are becoming faster, more reliable, more accessible and more user-friendly – advancements that apply in the healthcare industry as well as in manufacturing, retail, real estate, etc. Improvements in data processing speed, storage and transfer are fuelling the growth in online and streamed entertainment and news services in the same way that they are driving better imaging and radiology services. In other words, technology is expanding and improving in healthcare as much (and as little) as in any other field.

That said, certain technologies have seen rapid growth within the healthcare space, including:

- health-promoting mobile apps and wearables such as continuous glucose monitors, fitness apps, and digital virtual assistants and natural language processing tools;
- telemedicine solutions, including behavioural health counselling, substance abuse treatment, primary care, cardiology and management of chronic disease;
- robotics;
- artificial intelligence (AI) and machine learning (ML);
- genetic sequencing and personalised medicine;
- clinical decision-support software; and
- the internet of things (IoT), and more.

1.4 Emerging Legal Issues

In virtually every industry, technology-related legal issues follow a similar pattern: researchers and scientists develop new technologies; businesses and investors move quickly to commercialise these solutions; and legislators and regulators struggle to keep up. Where laws and rules are enshrined, they often occur after the proverbial horse has left the barn.

With respect to digital health in particular, there are two areas of growing concern for lawmakers and regulators:

- data privacy and security; and
- AI and ML.

Federal legislation regarding the privacy of healthcare data (sometimes referred to as “protected health information” or “personal health information”, both using the acronym PHI) has been in existence for several decades. The two main laws that govern the collection and use of PHI are the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

At the state level, a number of states are enacting laws to further protect personal information. While many such laws are more consumer-focused, cover a broad range of data types and are not exclusive to health information, per se, they typically contain language that applies to PHI. Major examples of such legislation include:

- the Biometric Information Privacy Act in Illinois;
- the California Consumer Privacy Act, the Genetic Information Privacy Act and the California Privacy Rights Act; and
- Virginia’s Consumer Data Protection Act.

With respect to AI and ML in digital health, significant attention has been paid to the use of these technologies in patient triage, communications between patients and providers (including so-called chatbots), data mining and analysis, and clinical decision support systems. The public release of OpenAI and other systems has likewise increased public awareness of the benefits and pitfalls of AI, at least in its current state. While lawmakers are beginning to hold hearings on the opportunities and challenges of using AI for a broad range of purposes, very little action has been taken to limit or regulate the use of these technologies. For supporters of AI technology, this means that developers will have an opportunity to move quickly and profit from their inventions; for critics, this means that the AI "seeds of destruction" are already being sown.

1.5 Impact of COVID-19

The COVID-19 global pandemic created an unexpected stress test for digital health solutions, with particular respect to telehealth/telemedicine. Immediately before and following the declaration of the public health emergency (PHE), federal and state agencies quickly announced measures to temporarily limit restrictions on the use of telemedicine and the technologies that support it, and noted that they would use their enforcement discretion to decline to enforce certain requirements.

Among other federal efforts, the FDA announced that it would allow manufacturers of certain FDA-cleared, non-invasive vital-sign measuring devices and clinical decision support software to modify their technology, claims or functionality to facilitate remote monitoring and home use of such devices without obtaining additional clearance for the modifications or expanded indications. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) likewise provided clarification on reduced enforcement and the waiver of prior regulations governing certain patient data privacy regulations, as well as expanded reimbursement for the use of telemedicine and related tools and technologies. Similarly, state and local agencies across the United States issued guidance allowing for increased use of telemedicine.

Although the US federal PHE has officially ended, federal, state and local regulators have acknowledged many of the benefits that accrued as a result of digital health tools. Many of the emergency use authorisations extended to certain medical devices during the pandemic have been allowed to continue on a temporary basis; US Centers for Medicare and Medicaid Services (CMS) reimbursement codes for telehealth services have been extended until 31 December 2023; and states across the country are taking rapid action to make permanent what were temporary exceptions to regulations, in order to expand the availability and use of effective digital health solutions.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

At the federal level in the United States, HHS is responsible for enhancing the health and well-being of all Americans and for fostering sound, sustained advances in the sciences underlying medicine, public health and social services.

Within HHS, the FDA is tasked with administering and enforcing the provisions of the Federal Food, Drug, and Cosmetic Act (FFDCA), which is the primary legislation that governs the manufacture, sale and use of products classified as food, dietary supplements, drugs and cosmet-

ics, including digital health products that meet the definition of medical devices.

Within the FDA, the Digital Health Center of Excellence provides regulatory advice and other support with respect to digital health policy, cybersecurity of medical devices, clinical studies, regulatory review support and co-ordination, AI and ML, strategic partnerships, and more. The FDA concentrates its digital health enforcement efforts on the safety of SaMD and other solutions, with an emphasis on patient safety.

Other key agencies within HHS that play a role in the regulation of digital healthcare include:

- the CMS, which has oversight of the Medicare programme, the federal portion of the Medicaid programme, the Children's Health Insurance Program, the Health Insurance Marketplace and related quality assurance activities;
- the Agency for Healthcare Research and Quality, whose mission is to produce evidence to make health care safer, higher quality and more accessible, equitable and affordable, and to work within HHS and with other partners to make sure that the evidence is understood and used;
- the Centers for Disease Control and Prevention (CDC), which provides leadership and direction in the prevention and control of diseases and other preventable conditions, and the federal response to public health emergencies;
- the National Institutes of Health, which supports biomedical and behavioural research in the United States and abroad, conducts research in its own laboratories and clinics, trains promising young researchers and promotes the collecting and sharing of medical knowledge;
- the OCR, which, among other responsibilities, ensures that individuals can access and trust the privacy and security of their health information; and
- the Office of the National Coordinator for Health Information Technology, which provides counsel for the development and implementation of a national health information technology framework.

On 29 December 2022, the Consolidated Appropriations Act of 2023 was signed into law. Section 3305 of the act, "Ensuring Cybersecurity of Medical Devices," amended the FFDCA by adding Section 524B. Effective as of 29 March 2023, a sponsor of a premarket submission for a cyber device must include information to demonstrate that the cyber device meets the cybersecurity requirements in Section 524B(b) of the FFDCA.

With respect to health information privacy, HIPAA does not require providers to report on their cybersecurity measures; however, HHS does publish a range of guidance with respect to administrative, physical and technical PHI safety measures, remote and mobile use of PHI, and so forth. Things change when a data breach occurs, however; in the event of a breach affecting 500 or more patients, the HIPAA Breach Notification Rule requires covered entities to notify affected patients, HHS and, in some cases, the media. Such notifications must occur without reasonable delay and no later than 60 days after discovering the breach. Notifications of breaches that affect fewer than 500 patients can be reported to HHS annually. The Breach Notification Rule also requires business associates to notify a provider of breaches at or by the business associate.

The HHS OCR enforces the HIPAA Privacy, Security and Breach Notification Rules, violations of which may result in civil monetary pen-

alties. In some cases, US Department of Justice-enforced criminal penalties may apply. Common violations include:

- unpermitted PHI use and disclosure;
- use or disclosure of more than the minimum necessary PHI;
- lack of PHI safeguards;
- lack of administrative, technical or physical ePHI safeguards; and
- lack of patients' access to their PHI.

2.2 Recent Regulatory Developments

Given the influx of investment dollars into digital health solutions, as well as increased research, development and commercialisation activity, state-level corporate practice of medicine laws and regulations are gaining importance. Corporate practice of medicine laws are aimed at avoiding the commercialisation of the practice of medicine, minimising potential conflicts of interest between corporations' shareholders and physicians' obligations to their patients, and preventing interference with practitioners' medical judgement.

This gives rise to a number of potential issues, particularly as they relate to the employment and management of physicians who provide telemedicine and other virtual health services across multiple jurisdictions. For example, digital health solutions involve patient triage and care decisions, which may raise questions with respect to physician independence when diagnosing and treating medical conditions. Complicating matters, state corporate practice of medicine doctrines vary between states, which means that hospitals, health systems and other organisations must identify and make efforts to accommodate the strictest legal requirements in the geographic regions in which they operate.

Since the US Supreme Court's decision in Dobbs, in which it overturned Roe v Wade, declared that the US Constitution does not provide a right to abortion and returned the authority to regulate abortion to the states, a patchwork system of legislation and regulation has been developed and is being actively litigated. One of the major effects of these new laws is to restrict the ability of individuals to access – and the ability of physicians, pharmacists and other practitioners to provide – reproductive medicine and maternal care services, particularly medication-based abortions (a significant number of which are managed via online prescription services and telehealth).

2.3 Regulatory Enforcement

A growing area of focus for regulators and law enforcement officials, particularly at the federal level, is telehealth fraud and overutilisation. In September 2022, the HHS Office of Inspector General (HHS-OIG) issued guidance identifying Medicare provider billing practices that it saw as being high risk. In April 2023, HHS-OIG followed up and issued a new toolkit and framework that would enable public and private entities, health plans, state Medicaid fraud units and federal healthcare entities to conduct internal audits and self-assessments, self-report potential violations, and work with agency officials to take corrective action and potentially reduce penalties.

While there is no clear evidence that digital medicine processes and billing methodologies lead to higher rates of fraud, as compared to in-person care delivery, the expanded use of telemedicine services is likely to increase the value of total, fraud-derived reimbursements. In other words, if one in every thousand billing physicians is a bad apple, after doubling the amount of such physi-

cians it is likely there will be two bad apples in the newly expanded population.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

Among non-healthcare regulators that nonetheless have some oversight responsibility for digital health products, perhaps the most important of these – at the US federal level – is the Federal Trade Commission (FTC). Primarily a consumer protection agency, the FTC focuses its efforts in the digital health space on the enforcement of product safety, compliance with advertising laws, and other issues with respect to health-related products and devices.

At the state level, attorneys general have begun working together to call for fitness and health application developers, large tech companies and other solution providers to strengthen data privacy protections. For example, in 2022 and following the Supreme Court's decision in Dobbs, a group of state attorneys general requested that Apple add new protections for reproductive health data collected and used by third-party apps made available on the company's App Store.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

Preventative care focuses on evaluating an individual's current health, preventing disease and providing routine care such as check-ups, annual wellness visits, immunisations and preventative screening tests. Preventative care is often provided at no cost, and the types of tests that fall under the umbrella of preventative care are typically based on recommendations from the United States Preventive Services Task Force.

On the other hand, diagnostic care usually involves investigating and/or treating a specific health issue, and may include management of symptoms, assessments of risk factors, ongoing care for chronic illnesses, and lab or other tests used to manage and/or treat a medical issue or health condition. Diagnostic care is typically paid for, to at least a certain degree, by the insurer, although insureds might owe money for deductibles, copays and/or coinsurance.

The Affordable Care Act (also known as Obamacare, or ACA) requires private health plans to cover services provided under four broad categories:

- evidence-based screenings and counselling services that have a rating of "A" or "B" in the current recommendations of the US Preventive Services Task Force;
- routine immunisations;
- preventative services for women; and
- preventative services for children and youth.

4.2 Increased Preventative Healthcare

As the US population ages, a number of "lifestyle-related" illnesses are on the rise, such as obesity, diabetes, hypertension, osteoporosis, Alzheimer's disease, dementia and other conditions. At the same time, decades-long changes in population behaviour, including eating habits, work schedules, use of technology to streamline or reduce manual labour, substance abuse and low-activity lifestyles, are increasing the prevalence of these conditions in younger populations as well.

Much of the growth in the digital health space is a result of efforts to reverse these trends. Wearable and handheld devices are being marketed to promote health-sustaining behaviours and combat unhealthful activities. Among other incentive-based digital health tools, insurance companies are establishing online and app-based self-reporting tools and offering financial discounts on premiums and other "rewards" for working out regularly at pre-screened gyms and fitness facilities. Healthcare providers, insurers, public health agencies and ancillary health-and-fitness organisations are also creating streaming webinars and online content aimed at educating consumers about fitness issues, and manufacturers are increasingly developing connected devices (stationary bikes, workout equipment, etc) that deliver real-time workouts and track fitness data over time.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Health, wellness and fitness data is subject to a broad range of data privacy, security and breach notification regulations, as described in **2.1 Healthcare Regulatory Agencies**. With respect to HIPAA, PHI includes any information in the medical record or designated record set that can be used to identify an individual and that was created, used or disclosed in the course of providing a healthcare service such as diagnosis or treatment.

The following 18 identifiers have been specified:

- patient names;
- geographical subdivisions smaller than a state, including street address, city, county, precinct, zip code and their equivalent geocodes;
- all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, etc, with some restrictions;
- telephone numbers;
- fax numbers;
- email addresses;
- Social Security numbers;
- medical record numbers;
- health plan/insurance beneficiary numbers;
- account numbers;
- certificate/licence numbers;
- vehicle identifiers and serial numbers, including licence plate numbers;
- device identifiers and serial numbers;
- digital identifiers, such as web universal resource locators (URLs);
- internet Protocol (IP) addresses;
- biometric identifiers, including finger, retinal and voice prints;
- full-face photographic images and any comparable images; and
- any other unique identifying number, characteristic or code.

Along with information on the above list, other data that can be associated with a particular individual that may be collected by hardware, software, an app or some other method that does not meet the FDA's definition of a medical device may still be subject to other federal and state privacy laws and regulations.

4.4 Regulatory Developments

As one of the largest and most consequential pieces of healthcare legislation of the past several decades, the ACA stands out for its provisions aimed at supporting preventative healthcare. Among other areas, the ACA requires insurance plans to cover a range of preventative services, including immunisations and vaccinations, screenings and counselling without requiring

copays, deductibles or other cost-sharing payments from insured patients. By supporting the implementation of state health insurance marketplaces, the ACA also expanded access to healthcare, the result of which was to enable patients and providers to identify potential risks and existing medical issues earlier in their progression, thereby improving outcomes.

The CDC also plays a major role in pursuing public health research and initiatives, as does the CMS; these focus on providing healthcare coverage and services to older and lower-income individuals and families, respectively. State health departments and Medicaid programmes also serve as an important backstop against the spread of disease and the promotion of health and wellness.

A significant effect of the expiration of the US federal PHE is that millions of Medicaid recipients across the country will no longer be eligible for healthcare benefits, which could cause an upsurge in otherwise preventable illness.

4.5 Challenges Created by the Role of Non-healthcare Companies

One of the most interesting developments in healthcare delivery is the entrance of "big box" retailers into the marketplace, such as Amazon, CVS, Walgreens, Best Buy and other companies. These and other entities are launching or acquiring primary care, urgent care, specialty care, pharmacy, in-home health, telehealth and other services – often disrupting traditional methods for providing healthcare.

In addition to giving rise to corporate practice of medicine concerns (see **2.2 Recent Regulatory Developments**), these new enterprises are creating anxiety about the weakening of data privacy and security protections. For example, a May 2023 article in The Washington Post ("To become an Amazon Clinic patient, first you sign away some privacy") noted that, at the time of writing, Amazon Clinic's authorisation form requests patients' approval for the "use and disclosure of protected health information", authorises Amazon to access one's "complete patient file" and notes that the information "may be re-disclosed", at which point it "will no longer be protected by HIPAA". Of course, there is no negotiation: either the would-be patients accept Amazon's terms or they go elsewhere for healthcare services. Among its rationale for seeking permission to sidestep HIPAA protections, Amazon claims that it is not a "healthcare" provider but is, instead, a provider of storefront software that directs patients to outside healthcare providers.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

With nearly one third of the world's data volume generated by the healthcare sector (and with the annual growth rate of healthcare data expected to reach 36% by 2025), the internet of medical things (IoMT) is poised to become a major contributor to this information surge. IoMT devices range from those that monitor blood glucose, heart rate, depression, Parkinson's disease and other disease states, to so-called smart pills with microscopic sensors that can travel through a patient's digestive system.

Key concerns about connected devices include data privacy, cybersecurity and patient safety. Providers must ensure that processes are in place to address device failures, lack of con-

nectivity, data hacking and other potential risks. Management of such risks requires patients to accept a higher level of responsibility for their own care, which may not be appropriate for all individuals or for all conditions.

5.2 Legal Implications

At the present time, there are no specific legal regimes focused on liability for adverse health outcomes relating to wearable, implantable or digestible medical devices that can be described as "connected" or IoMT. However, broader legal frameworks that can be brought to bear include federal and state product liability laws, medical malpractice laws, FDA oversight of medical and healthcare products, and HIPAA, HITECH and other data privacy and information security laws described elsewhere in this article.

Medical device reporting is one of the post-market surveillance tools used by the FDA to monitor device performance, detect potential safety issues and contribute to risk-benefit assessments of these products. Manufacturers, device user facilities, importers and other "mandatory reporters" are required to submit certain types of reports for adverse events and product problems about medical devices to the FDA. The FDA also encourages healthcare professionals, patients, caregivers and consumers to submit voluntary reports about serious adverse events that may be associated with a medical device, as well as use errors, product quality issues and therapeutic failures.

The Voluntary Malfunction Summary Reporting programme was established in 2018 and allows eligible manufacturers to report certain device malfunction medical device reports for certain kinds of devices and malfunctions. These are made in summary form on a quarterly basis. Healthcare professionals, patients, caregivers and consumers can submit voluntary reports to MedWatch, the FDA's Safety Information and Adverse Event Reporting Program.

5.3 Cybersecurity and Data Protection

Interconnected medical devices can deliver numerous benefits that increase the ability of physicians and other practitioners to deliver high-quality care, expand patient access to various prevention, diagnostic and treatment modalities, and improve healthcare outcomes. However, they do give rise to specific information-security risks and vulnerabilities, some of which may be determined by the specific nature of the computing environment.

With respect to cloud-based computing, for example, medical data and services are typically hosted and managed by third-party service providers. Significant threats include data breaches, unauthorised access, data loss and other provider-specific vulnerabilities. With respect to on-premises and local computing environments, key cybersecurity risks include device vulnerabilities (allowing for exploitation by attackers), insider threats (eg, unauthorised access to, misuse of, or theft of devices and/or data, whether by malicious intent or negligence), network vulnerabilities (eg, weak authentication protocols or unencrypted communications channels), failure to apply security patches and updates, physical theft of devices, and compromised device integrity.

Risk-mitigation strategies include strong, clear terms in vendor contracts that outline specific cybersecurity roles and responsibilities, the implementation of strong encryption and protocols, ongoing security assessments and, perhaps most important, staff training.

5.4 Proposed Regulatory Developments

Healthcare and information security regulation is an ongoing process. A number of federal government agencies provide guidance on health information privacy, cybersecurity and medical devices. The Computer Security Resource Center of the National Institute of Standards and Technology (NIST –part of the US Department of Commerce) has published dozens of "800 Series" special publications that focus on computer/information security across a range of industries, including healthcare, as well as "1800 Series" cybersecurity practice guides, NIST internal reports and Information Technology Laboratory bulletins that give wide-ranging advice on establishing, governing and managing information and communications technology risks.

Similarly, the FDA and its Digital Health Center of Excellence provide extensive information and have published numerous regulatory guidance documents on digital health-specific issues, including software functions, mobile medical applications, updates to medical software policies resulting from Section 3060 of the 21st Century Cures Act, medical device data systems, medical image storage devices, medical image communications devices, clinical decision-support software, and more.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

The FDA uses the definition of SaMD provided by the International Medical Device Regulators Forum (IMDRF): "software intended to be used for one or more medical purposes that performs these purposes without being part of a hardware medical device."

The IMDRF is a global, voluntary group of medical device regulators pursuing the harmonisation of medical device regulation. In 2013, IMDRF formed the Software as a Medical Device Working Group to develop guidance supporting innovation and timely access to safe and effective SaMD globally. Chaired by the FDA, the working group agreed upon the key definitions for SaMD, a framework for risk categorisation of SaMD, the Quality Management System for SaMD, and the clinical evaluation of SaMD.

In the United States, nearly 2,000 distinct types of medical devices have been categorised by the FDA into either Class I, Class II or Class III, based on the level of control necessary to ensure the safety and effectiveness of the device. Class I devices are viewed as the least risky; Class III includes devices that pose the greatest risk.

The regulatory controls for each device class include:

- Class I (low to moderate risk): general controls;
- Class II (moderate to high risk): general controls and special controls; and
- Class III (high risk): general controls and premarket approval.

Most Class I and II devices are exempt from premarket notification (501(k)) requirements, and may also be exempt from current Device Good Manufacturing Practices requirements under the Quality System Regulation. However, exempt devices must still comply with other general regulatory controls relating to the registration of producers of devices, banned devices, notifications and other remedies, records and reports on

devices (including adverse event reporting and device tracking), and other general provisions with respect to the control of devices intended for human use.

Special controls for Class II devices are usually device-specific and include performance standards, post-market surveillance, patient registries, special labelling requirements, pre-market data requirements, and other guidelines.

Pre-market approval is required of Class III devices that are intended to be used in supporting or sustaining human life or preventing the impairment of human health, but which may present a potential, unreasonable risk of illness or injury for which general and special controls are insufficient to provide reasonable assurance of the safety and effectiveness of the device, or for which there is insufficient evidence to make such a determination.

Regulators acknowledge the speed of innovation within SaMD and are pursing ongoing efforts to improve the various processes involved in regulating these important healthcare tools.

7. Telehealth

7.1 Role of Telehealth in Healthcare

In recent years (before and during the COVID-19 global pandemic), it has become increasingly clear that telemedicine has earned its place in the pantheon of care-delivery methodologies available to practitioners and patients. Telemedicine stands out from in-person treatment in the way that it can offer rural communities, colleges and universities, major employers, chronically ill or homebound individuals, underserved populations, and patients in general (even during non-pandemic times) effective diagnostic, prevention and treatment services.

Telehealth in the future will be on its strongest footing when advocates and users recognise that one-size fits all solutions are better described as "one size fits none". As hospitals, health systems, clinics and other providers apply the lessons learned during the COVID-19 pandemic to their own long-term objectives – including quality of care and cost-effectiveness – telemedicine will cement its position as a cornerstone of healthcare delivery.

Providers can take the following actions now to help make the most effective use of telemedicine in the long run:

- require the same standard of care for telehealth visits as for in-person visits;
- understand when telemedicine is appropriate and when it is not;
- share information, data and best practices at the industry level;
- develop strategies to promote patient buy-in and engagement in telemedicine and personal health management;
- integrate artificial intelligence and other technologies to improve diagnostics and treatment; and
- work closely with state and federal regulators to resolve licensure, corporate practice of medicine and other regulatory issues.

With respect to the latter point, the Federation of State Medical Boards supports the Interstate Medical Licensure Compact, which is an agreement among 37 states, the District of Columbia and the Territory of Guam to work together to streamline the licensing process for physicians wishing to practise in multiple states. Similar licensing compacts are also gaining momen-

tum. Since the beginning of 2023, dozens of US states have passed or are actively pursuing legislation that allows participation in licensure compacts covering audiologists, speech pathologists, occupational therapists, mental health counsellors, and more.

7.2 Regulatory Environment

In the early months of the pandemic, HHS, the FDA, CMS and other federal agencies engaged in a co-ordinated effort to ease restrictions governing the use of telehealth and related digital health technologies. These included:

- waivers of certain HIPAA and HITECH non-compliance sanctions and penalties against covered entities and providers using telehealth and non-public facing technologies for remote communications (including good-faith use of video applications such as Zoom, Skype and FaceTime);
- waiver of the "originating site requirement", allowing Medicare beneficiaries to receive telehealth services anywhere and not just at a designated healthcare facility or rural site;
- waiver of the requirement that physicians and non-physician practitioners be licensed in the state where the patient is located (subject to certain conditions);
- waiver of the "relationship requirement, which, prior to the current national health emergency, meant that a provider or someone in the practice must have seen the patient in-person before initiating subsequent telehealth services;
- removal of limits on the number of times certain services can be provided by Medicare telehealth;
- encouragement for Medicaid programmes (which vary by state) to increase access to telehealth; and
- application of non-enforcement policies to situations where a plan or issuer adds benefits, or reduces or eliminates cost sharing, for telehealth and other remote care services.

Since the expiration of the federal PHE in early May 2023, many of the above exemptions and policies have been extended at least until 31 December 2023. A significant effort is being made at the federal level, and among the states, to make permanent these waivers as well as other digital health best practices that were introduced and/or stress tested during the pandemic.

7.3 Payment and Reimbursement

From a reimbursement perspective, the early pandemic initiatives emanating from federal agencies (see **7.2 Regulatory Environment**) also included:

- expanded telehealth codes for which providers can be reimbursed; and
- equalised payment rates such that in-person (facility) and telehealth visits are reimbursed at the same level.

CMS telehealth codes will remain in effect through the remainder of 2023, although it appears possible that expanded reimbursement for telehealth services and parity for telehealth and in-person services will be enshrined in forthcoming proposed and final rules.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

The IoMT enables providers to deliver more personalised care, support early detection of medical conditions, take advantage of remote moni-

toring of patients and improve overall patient outcomes. Key technological developments that have facilitated the creation and expanded use of connected devices, wearables, implantables and high-volume, high-speed data exchange and analysis include:

- high-speed internet connections and standardised protocols, including Wi-Fi, Bluetooth and cellular networks;
- technology miniaturisation, which has allowed for more effective implantable devices, such as insulin pumps and pacemakers, that can also transmit data wirelessly;
- AI and ML, which are capable of analysing large volumes of data, analysing patterns and offering predictive assistance that helps providers diagnose disease, identify potential disease outbreaks and disease vectors, and deliver precision medicine solutions;
- interoperability and data standards, which have allowed for seamless communication and data exchange (including electronic health records) between devices, systems, networks and platforms; and
- cloud-based data storage and computing, which support the collection and analysis of healthcare data from virtually anywhere.

As noted in **5.1 Internet of Medical Things and Connected Device Environment**, however, IoMT solutions give rise to a host of cybersecurity risks. Bad actors and cyberthreats are growing exponentially, and a number of hospitals and health systems have found themselves vulnerable to cyberattacks, data hacking, ransomware and other threats. Privacy advocates also call attention to the need to protect PHI wherever and however it is stored, used and transmitted, whether via apps on mobile devices, during telehealth visits, or through other activities relating to healthcare delivery.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

Any telecommunications technology that delivers increased speed and bandwidth and reduces latency is a win for healthcare in general, and for digital healthcare in particular. High-resolution imaging and file transfers, improved videoconferencing, emerging treatment modalities such as robot-assisted surgery, remote consultations between emergency-room staff and far-flung specialists, and more, all benefit from faster, more reliable networks.

Likewise, as healthcare research and clinical practice create ever-increasing volumes of data, the ability to share such information quickly and safely will further contribute to disease prevention and treatment modalities, whether conducting personalised medicine (also known as "precision medicine") to, eg, fight specific cancers in individuals, or developing, testing and implementing broad-scale public health strategies.

While the benefits of 5G networks are manifold, those who stand to see the greatest benefit are patients who live in – and practitioners who provide services to – rural, low-income and other under-served communities. In urban cities, high-speed broadband connections using digital subscriber lines, cable modems, fibre-optic technology and other technologies are widespread and relatively available to healthcare providers and patients alike. In rural, poorer communities, however, internet services may be limited and/or slow, requiring the use of wireless technologies. Connecting such communities to 5G networks can significantly increase access to care and improve the speed, delivery and quality of such care.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

In some respects, the growth of digital healthcare has had a minimal impact on the use and sharing of personal health information in clinical and research settings. Protected health information is protected health information, no matter how it is acquired, stored, used, shared or disposed of. In essence, paper records must comply with the same regulatory standards as electronic files.

That said, digital healthcare is, by definition, an information phenomenon, and the modalities, processes and technologies through which this information is gathered raise unique risks. Where, for example, data thieves were once required to physically break into a physician's office to steal or destroy files (significantly limiting the impact of such actions), today's remote hackers can reach virtually anywhere in the world and launch attacks that affect hundreds of thousands, even millions, of patient records at a single pass. Hospitals and health systems have been key targets for ransomware attacks, creating chaos for patients, providers and healthcare administrators, not to mention law enforcement and regulatory officials.

Although there are a number of global and national efforts to increase cybersecurity through consistent, well-documented standards, protocols and policies, most patients and providers operate within a patchwork of competing systems. Under these conditions, developers, vendors, suppliers and users of digital health technology must make an extra effort to scrutinise business partners' cybersecurity policies and practices, negotiate clear, comprehensive terms in contracts, collaborate to perform regular security maintenance, and quickly and completely notify relevant law enforcement and regulatory officials in the event of a data breach or cyberattack.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

The potential of AI in healthcare appears virtually limitless, but it is important to recognise that AI is far from flawless. Although AI solutions can offer unique opportunities to improve healthcare delivery and patient outcomes, AI-enabled medical products can and have resulted in inaccurate and possibly harmful treatment recommendations. Errors can be introduced through inaccurate or biased data used to build and train ML tools, through algorithms that give inappropriate weight to certain data points, and other flaws. Stakeholders across the spectrum – individual providers, health systems, technology developers, legislators, regulators and patients – must work together to ensure the effectiveness and safety of AI-driven healthcare technology.

To ensure accuracy and reliability, the datasets used to train AI algorithms must be large, diverse and unbiased. However, assembling such datasets can be complex and expensive, particularly given the fragmentation of the US healthcare system. A recent analysis of data used to train image-based diagnostic AI systems found that approximately 70% of studies that were included used data from three states, and that 34 states were not represented at all in the dataset. Similarly, if images used to train an algorithm to detect skin cancers consist primarily of patients with light skin tones, the AI may fail to detect – or over-detect – possible skin cancers in patients with darker skin tones. This is an important issue

when people of colour are already typically diagnosed later in the progression of skin diseases.

Furthermore, many AI programmes are referred to as "black box" systems because the datasets, calculations and techniques used to identify patterns and present results are too complex for even the programmers and developers to understand. If AI fails to perform as expected, it can be very difficult to identify why the failure is occurring.

For the time being, one of the basic tenets for using AI is that it may be used to "inform" decisions but must not be used to "make" or drive decisions. In addition, the FDA has outlined an approach to managing adaptive learning, based on four core principles:

- establish clear expectations on quality systems and good ML practices;
- conduct pre-market assessments of SaMD products;
- engage in routine monitoring of SaMD products to determine when an algorithm change requires FDA review; and
- embrace transparency and real-world performance monitoring.

11.2 AI and Machine Learning Data Under Privacy Regulations

AI and ML technologies are subject to the same data privacy regulatory frameworks that apply to all health-related products and services.

Other core concerns relating to the training and implementation of AI often revolve around:

- appropriateness (the process of deciding how the algorithm should be used in the local context and matching the ML model to the target population);
- bias (the systematic tendency of a model to favour one demographic group over another); and
- fairness (understanding the impact of AI on various demographic groups and choosing definitions of fairness that satisfy legal, cultural and ethical requirements).

In December 2022, the HHS OCR issued a bulletin noting that the collection of sensitive information via tracking technologies such as AI-driven Google Analytics and Meta Pixel, and stating that it is critical for regulated entities to ensure that PHI is only disclosed as expressly permitted or required by the HIPAA Privacy Rule. This bulletin followed a 2022 regulation proposed by the OCR explicitly prohibiting healthcare providers enrolled in Medicare from discriminating based on race, sex and other protected characteristics through the use of clinical algorithms in decision-making.

State-level regulatory oversight of AI is also happening in places such as California, where the state's attorney general initiated an ongoing probe into how algorithmic tools are exacerbating racial and ethnic disparities.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Many of the legal issues facing companies operating in the digital healthcare space have been described elsewhere in this document. The following are additional, emerging issues of which such companies should be aware.

- Increased federal antitrust enforcement – following the lead of President Biden, who launched his administration by singling out

anti-competitive activity and consolidation in the US hospital and health systems marketplace as a primary cause of reduced access to healthcare services, particularly in rural communities, the US Department of Justice and FTC have been aggressively pursuing the application of antitrust law to the healthcare sector. As large retailers such as Amazon, Best Buy, CVS and Walgreens expand their service lines, it is likely that such scrutiny will only increase.

- Uncertainty regarding implementation of the No Surprises Act – in February 2023, HHS announced a temporary halt to reimbursement decisions under the National Security Agency while it reviewed a court ruling that vacated portions of the implementing regulations and held that independent dispute resolution between providers and payers for reimbursement of out-of-network services unfairly favoured payers.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

In its 2021 forum on the Future of Digital Healthcare after COVID-19, the Organisation for Economic Co-operation and Development determined that "the main barriers to building a 21st century healthcare system are not technical, but can be found in the institutions, processes and workflows forged long before the digital era". Simply put, a digital healthcare system cannot work if it is simply laid on top of aging infrastructure designed to support traditional care delivery.

Understanding that investment in infrastructure is necessary to realise the full transformative potential of digital health, some countries (including Australia and the UK) have committed billions of dollars toward building new – and reinforcing existing – systems and platforms. In the United States, however, a recent study by the American Society of Health Engineers, which examined financial measures that demonstrate how well hospitals are keeping their facilities current, found that facilities are not just out of date – they are degrading at an increasing pace.

Key principles to keep in mind when preparing infrastructure for a future, digital information-dependent healthcare system include maintaining a focus on human-centred design and sustainability and the creation of innovative spaces that enable the integration of innovative technologies. Healthcare companies must invest now in an infrastructure that should not quickly face an inevitable replacement, but have the capacity to evolve as rapidly as the technologies that support them.

13.2 Data Management and Regulatory Impact

In December 2022, CMS issued a proposed rule that would improve patient and provider access to health information and streamline processes related to prior authorisation for medical items and services. The proposed rule includes requiring implementation of a Health Level 7® (HL7®) Fast Healthcare Interoperability Resources® (FHIR®) standard Application Programming Interface (API) to support electronic prior authorisation. Other policy proposals include:

- expanding the current Patient Access API to include information about prior authorisation decisions;
- allowing providers to access their patients' data by requiring payers to build and maintain a Provider Access FHIR API, to enable data exchange from payers to in-network providers with which the patient has a treatment relationship; and

- creating longitudinal patient records by requiring payers to exchange patient data using a Payer-to-Payer FHIR API when a patient moves between payers or has concurrent payers.

With respect to cybersecurity, the FTC, FDA, Department of Transportation, Department of Energy, Securities and Exchange Commission, Cybersecurity and Infrastructure Security Agency and other federal agencies are all working on the development of new regulations and enforcement activity. Throughout the past 18 months, nearly every US state has enacted cybersecurity legislation. Although this activity does not target the healthcare industry specifically, the bulk of this new legislation and rulemaking will have an impact on payers, providers and patients.

Another area of focus is the creation of "software bills of materials" that enable companies to quickly and accurately identify and manage all of the various software programs embedded in their increasingly complex computer systems and platforms. This can help vendors and users identify vulnerabilities that arise from multiple layers of software bundling.

14. Intellectual Property

14.1 Scope of Protection

Today's software programs are no longer the product of a lone inventor or programmer, sitting in a cold garret or garage and quietly working away at the product of the century. Rather, technology development often involves far-flung partnerships across multiple borders and time zones. Digital health products often comprise numerous distinct inventions brought together to create a unique product. Technology transfers, outsourcing and joint development agreements, public-private partnerships and more are increasingly creating a complex web of intellectual property right claims and disputes.

Add one more wrinkle to the mix: if an AI program creates an invention, who owns it? In declining to hear an appeal by computer scientist Stephen Thaler challenging the US Patent and Trademark Office's refusal to issue patents for inventions created by an AI algorithm, the US Supreme Court agreed with the US Court of Appeals for the Federal Circuit in saying "It's not the AI". The courts agreed that patent law unambiguously requires inventors to be human beings.

Given the complexities of intellectual property law and ownership, it is impossible to lay out the multiple issues at play in determining ownership of IP rights, including trade marks, copyrights and patents. Companies operating in the digital health space should work closely with experienced legal counsel to identify, protect and license any health-related technologies they develop.

14.2 Advantages and Disadvantages of Protections

Intellectual property protection confers specific and limited legal rights and safeguards to protect inventors' investments of time and resources, and stimulate broader economic growth. In the United States, the following forms of IP protection are available, each of which has certain advantages and disadvantages.

- Patents grant inventors exclusive rights to their inventions and disallow other parties from making, using or selling the patented invention. Filing for a patent requires disclosure of the details of an invention that can add to the growing body of technological know-how and increase scientific knowledge. However, patent application processes are

costly, complex and time-consuming, and patents have a limited duration, after which the invention enters the public domain.
- Copyright protection is granted automatically upon the creation of an original work, and does not require registration (although, in many cases, registering a copyright helps to prevent or minimise potential disputes). Copyright holders have exclusive rights to reproduce, display, market or modify their works. While encouraging creativity and offering economic incentives, copyrights do not extend to ideas, facts or concepts – only the unique expression of these ideas. And while copyright protection generally lasts for the lifetime of the creator (and sometimes beyond that timeframe), the fair-use doctrine does allow others limited use of copyrighted works without permission.
- Trade marks protect brands, logos and other signs that differentiate products and services, and help companies build or increase their profile and customer loyalty. The trade mark registration process can also be expensive and time-consuming, and trade marks offer only limited protection.
- Trade secrets can be protected indefinitely, as long as the information remains secret or confidential. Trade secret protection does not require registration and can protect a wide range of formulas, processes, customer and vendor lists, business strategies and more. However, once a trade secret is exposed, it loses its protection. Legal remedies for trade secret misappropriation can be difficult to enforce, and the recovery of damages is often challenging.

14.3 Licensing Structures

Several licensing structures can be applied in the context of digital healthcare that allow for the lawful and controlled use of relevant IP. Such structures include:

- end-user licence agreements, also known as terms and conditions;
- data licensing agreements, involving patient health records, research data, etc;
- software as a service agreements, often used in the context of cloud-based solutions;
- IP licensing agreements, involving patents, copyrights, trade marks and trade secrets, and defining the rights granted by IP owners to licensees; and
- supplier and vendor agreements, often used when multiple parties contribute hardware, software or services to the creation of an end product – they frequently include terms covering warranties, licensing, liability and dispute resolution.

14.4 Research in Academic Institutions

According to the World Intellectual Property Organization (WIPO), a self-funding agency of the United Nations, effective IP policies and agreements between universities and research institutions, physician/inventors and private sector digital health technology companies should seek to provide structure, predictability and a beneficial environment in which partners and stakeholders can access and share knowledge, technology and intellectual property. WIPO maintains a database of institutional IP policies that provide examples from different institutions across the globe and help users understand options and alternatives for dealing with IP issues.

Key stakeholders typically include:

- universities and research institutions;
- employees of these institutions;
- inventors' research groups and departments;

- graduate and post-graduate students;
- post-graduate and post-doctoral fellows;
- visiting researchers;
- sponsors and industry collaborators;
- national patent offices;
- funding agencies;
- industry representatives; and
- government representatives.

14.5 Contracts and Collaborative Developments

Every collaboration is unique, and relevant contracts should take into account the specific requirements and goals of all parties involved in the contract. In addition to obtaining legal and expert advice, the following are some best practices when negotiating contracts:

- define project objectives and scope clearly;
- determine ownership and rights to the IP developed during the collaboration – among other options, IP may be jointly owned, individually owned, or licensed to one or more parties;
- allocate collaborators' contributions and responsibilities, including financial arrangements;
- establish clear decision-making processes and accountability;
- take regulatory compliance into account; and
- identify and address potential challenges, risks, disputes, etc.

15. Liability

15.1 Patient Care

Theories of liability arising out of medical decisions based on digital health technologies, including AI, ML, SaMD and data analytics, include the following.

- Medical malpractice, potentially arising out of a failure to critically evaluate AI recommendations and deviating from the standard of care. Health systems that employ physicians and other practitioners may also be liable for practitioner errors.
- Other negligence, possibly implicating physicians, health systems, hospitals and medical practices that all play a role in and have some responsibility for the well-being of patients. This could include, for example, making a poor choice of an AI solution because it has been trained on a database and/or population information from a demographic group different from the patient (or patients) receiving care.
- Products liability, in which poor design, manufacturing defects or failure to warn about potential risks lead to injury. Current case law in this area, with respect to digital health, remains unsettled.

15.2 Commercial

During the COVID-19 pandemic, force majeure became a hot-button topic as businesses across industries were forced to address supply chain disruptions, labour shortages, remote work, cybersecurity threats and other issues that negatively affected organisational performance – including their (and their business partners') ability to fulfil contract terms.

Depending on the circumstances of the matter, negligence, breach of contract, strict liability, vicarious liability, warranty claims, fraud or misrepresentation and other theories of liability may come to bear in the dispute. Given the unique nature of each matter, it is important to seek effective, experienced counsel in order to identify and pursue effective remedies.

Trends and Developments

Contributed by:
Nadia de la Houssaye, Allison Bell, Keiana Palmer and Chino Onubogu
Jones Walker LLP

Jones Walker LLP is among the largest law firms in the United States, with more than 350 attorneys across the Southeast and other strategic locations, including Miami, New York City and Washington, DC. Led by a core group of veteran healthcare attorneys, the firm's healthcare industry team includes attorneys from all of the firm's major practice areas, who all have extensive experience in specific practice areas, as well as in-depth knowledge of today's healthcare marketplace and regulatory environment. Jones Walker's nationally recognised digital health and telemedicine team has been actively assisting healthcare entities with the structuring and integration of telemedicine systems for more than 20 years. These healthcare entities range from large hospital systems that cross state borders to hospital-based physician practices, direct-to-consumer telemedicine providers, and manufacturers of medical devices used in telemedicine monitoring and diagnoses.

Authors

Nadia de la Houssaye is a partner in Jones Walker' litigation practice and co-leader of the healthcare industry team. She works extensively with hospitals, health systems, providers and start-up companies to structure and integrate telemedicine, telehealth and digital health platforms. Her passion for the expansion and growth of telemedicine began in 1997, when she co-created and helped launch one of Louisiana's first teleradiology networks. Since 2004, Nadia has provided strategic counsel to healthcare providers and hospital systems on telemedicine service lines, including international telemedicine arrangements involving multistate and international licensure and scope of practice issues, cross-border compliance issues, patient consent requirements, commercial payor reimbursement issues, Medicare and state Medicaid billing requirements, and coverage and reimbursement issues.

Allison Bell is a partner in the Jones Walker corporate practice group, and co-leader of the healthcare industry team. She has extensive experience in advising public and private healthcare providers and companies in acquisition and divestiture transactions, mergers, joint ventures and other complex business transactions. Allison also represents not-for-profit and for-profit healthcare providers in unique healthcare-related transactions, including joint operating agreements and complex strategic affiliations. She currently represents the largest health system in Louisiana.

Contributed by: Nadia de la Houssaye, Allison Bell, Keiana Palmer and Chino Onubogu, **Jones Walker LLP**

Keiana Palmer is an associate in Jones Walker's corporate practice group and represents private and public companies, institutional investors and other clients in a wide range of corporate and commercial law matters. She has experience in advising high-growth digital health and technology start-ups on entity formation and conversion, corporate governance, regulatory compliance, risk management and strategic planning, among other matters. She has also represented organisational stakeholders; reviewed, drafted and negotiated a variety of commercial contracts; and assisted a range of clients with corporate transactions.

Chino Onubogu is an associate in the Jones Walker corporate practice group, and provides broad-ranging counsel to clients across the country with interests and operations in diverse industries, including healthcare and technology. Chino has experience in drafting corporate agreements, technology transactions and regulatory opinion letters for digital start-ups and healthcare practices. She has also assisted clients with various corporate matters, including corporate governance, multistate entity formation and licensing, entity conversions, data privacy compliance (HIPAA, federal and state), digital implementation of services, and corporate practice of medicine issues.

Jones Walker LLP

201 St. Charles Ave
New Orleans
LA 70170-5100
USA

Tel: +1 504 582 8000
Fax: +1 504 582 8583
Email: ndelahoussaye@joneswalker.com
Web: www.joneswalker.com

Contributed by: Nadia de la Houssaye, Allison Bell, Keiana Palmer and Chino Onubogu, **Jones Walker LLP**

Digital Healthcare in the USA: an Overview

Digital health: lessons learned during the pandemic are paving the way forward

On 11 May 2023, the United States allowed the federal COVID-19 public health emergency (PHE) to expire. A week before that, on 5 May, World Health Organization Director-General Tedros Adhanom Ghebreyesus declared "an end of the public health emergency of international concern".

Although most agree that COVID-19 is still very much in the picture, the new stance of international and US federal and state officials is a clear signal that many are also ready to treat the disease as a back-burner issue simmering on low boil, and to refocus attention, resources and money on other concerns. Whether or not this is a wise policy is subject to debate: Some argue that reduced vigilance will open the door to opportunistic variations of the coronavirus and cause a new or resurgent pandemic. Others insist that we have the tools, knowledge and treatments to limit infections and must now work to address the longer-term economic, educational and other consequences of several years of lockdowns.

With respect to digital health and telemedicine, however, there are encouraging signs that the lessons learned during the pandemic will have a longer shelf life. Digital health solutions played a major role in providing cost-effective, high-quality healthcare to Americans across the country and from all backgrounds. Rural and underserved populations, in particular, benefitted from the loosening of federal and state restrictions on telehealth, physician licensure and other rules that often served as barriers to the delivery of modern healthcare.

In a July 2022 report, members of global consulting firm McKinsey & Company's Life Sciences Practice noted that "[d]igital technologies have the potential to play a critical role in efforts to improve health equity". In so doing, they pointed to the fact that investments in global health have contributed to approximately one third of all economic growth in advanced economies throughout the past century. To get to the next level, digital health solutions must be created and implemented that reach previously excluded or under-represented groups, increase access and address unmet needs – all while taking into account such communities' historical experience with the medical establishment.

Before continuing, it is important to state what is possibly (and hopefully) an obvious point: the goal of digital health – and of any healthcare discipline, for that matter – is to practise good medicine. Every cost-reducing, access-expanding, workflow-streamlining, data-protecting and outcome-improving technology solution must be directed toward this singular objective.

In a sign that things are headed in a positive direction now that the United States has reached the official end of the PHE, numerous federal and state lawmakers and agency officials are engaging in concerted, co-ordinated efforts to make permanent a number of pandemic-related digital health measures that, throughout the past three years, have had demonstrable, positive effects on care delivery and patient outcomes.

Within one week in May 2023, for example, Florida, Montana, Oklahoma and numerous other states either passed or moved through at least one of their legislative chambers legislation relating to:

- pharmacist prescribing authority exceptions;

- teledentistry treatments for patients in long-term care facilities;
- the use of audio-only calls for telehealth services;
- expanded use of telehealth to provide mental health services in schools; and
- the standardisation of records related to patient consent for treatment and data collection and sharing.

This work is not just the purview of legislators and regulators. To help achieve these and other goals, in January 2022 the American Telemedicine Association (ATA) announced a new affiliated trade organisation, ATA Action. Founding members of ATA Action include such well-known names in healthcare as LifePoint Health, Teladoc Health, HCA Healthcare and Intermountain Healthcare, as well as leading retail brands and other businesses, including Walmart, Philips and Best Buy Health. The organisation is working to support the enactment of state and federal telehealth coverage and appropriate payment policies to secure telehealth access for all Americans.

In this context, the following is a review of some of the key developments in the digital health space throughout the past year, with an eye toward the remainder of 2023 and beyond.

Licensure: growing acceptance of interstate compacts

Prior to the COVID-19 pandemic, most states had strict limitations on the licensing of healthcare professionals to practise telemedicine within their borders. Physicians and non-physician practitioners (including nurses, psychologists and physical therapists) were required to hold licences in the states where their patients resided. In certain states, "relationship requirements" also meant that the provider or someone in the provider's practice needed to examine the patient in person before initiating telemedicine services.

In early 2020, as the pandemic gained momentum, the Department of Health and Human Services issued a series of bulletins, notifications and FAQs announcing and then clarifying waivers of certain federal Health Insurance Portability and Accountability Act (HIPAA) regulations and Health Information Technology for Economic Clinical Health (HITECH) Act non-compliance sanctions against covered entities and providers. As a result, state licensing boards, in turn, began to loosen their telemedicine licensing requirements.

With the expiration of federal and state PHEs, industry groups, elected officials and other advocates have strengthened their efforts to officially expand licensure opportunities for providers. For example, the Federation of State Medical Boards supports the Interstate Medical Licensure Compact (IMLC), an agreement among 37 states, the District of Columbia and the Territory of Guam to work together to streamline the licensing process for physicians wishing to practise in multiple states. More than 80% of US physicians are eligible to obtain licensures through the IMLC.

The IMLC is modelled after the Nurse Licensure Compact, which allows holders of a multistate nursing licence to practise in all of the 40 participating jurisdictions. However, a key distinction between the two compacts is that physicians must still pay between USD300 and USD700 for each state licence – a significant financial burden and ongoing expenditure for providers practising telemedicine at the national level.

Other such licensing compacts are also gaining momentum. For example, during the spring of

2023, states such as Missouri, Montana, South Carolina and Texas passed or were actively pursuing legislation that allows participation in compacts covering audiologists, speech pathologists, occupational therapists, mental health counsellors and more.

CMS telehealth codes to continue through 2023

Prior to 2023, major healthcare stakeholders had expressed fears that telehealth services made temporarily available during the pandemic would disappear once the PHE was ended. The US Centers for Medicare and Medicaid Services (CMS) has responded to this concern in several ways, including the following:

- for 2023, CMS added new Healthcare Common Procedure Coding System (HCPCS) codes to the list of Medicare telehealth services covering prolonged services and chronic pain management and treatment;
- CMS is retaining more than 40 codes on the Medicare Telehealth Services List until 31 December 2023; and
- telehealth claims may continue to be billed with a place-of-service indicator that would have been used had the service been billed for an in-person visit.

In so doing, CMS is:

- implementing the 151-day Medicare telehealth flexibilities that were contained in the 2022 Consolidated Appropriations Act (CAA), including allowing telehealth services to be furnished in any geographic area and in any originating site setting, including the beneficiary's home;
- allowing certain services to be furnished on audio-only telecommunications devices; and
- allowing physical therapists, occupational therapists, speech-language pathologists and audiologists to furnish telehealth services.

The CAA also delays the in-person visit requirements for mental health services furnished via telehealth for a full 152 days after the end of the PHE on 11 May 2023.

While these and other steps are encouraging, the future of telemedicine reimbursement will depend in large part on the ability of providers, insurers and states to continue to convince relevant officials of the ongoing value of digital health services.

Capital is flowing to digital health technologies

Beginning in early 2022, labour shortages, supply chain disruptions, rising inflation, increased interest rates and geopolitical tensions played a significant role in tamping down the US economy. But while no industry is fully recession-proof, the healthcare industry and the digital health technology sector in particular have shown astonishing resilience.

For example, in its twelfth annual Global Healthcare Private Equity and M&A Report, Bain & Company reported that 2022 was the second-best year for healthcare private equity investments, with USD90 billion in disclosed deal value, down somewhat from 2021 but a full USD10 billion above the next-highest year.

Digital healthcare and healthcare IT have seen a significant amount of activity, particularly in areas that can streamline workflows, reshape revenue cycle management, and manage and use life sciences and clinical data. Although traditional M&A activity has not shown a marked uptick, a number of digital health start-ups

announced significant capital-raising deals in early 2023, including USD375 million in new funding for Monogram Health, USD203 million for Paradigm, USD300 million for ShiftKey and USD200 million for ShiftMed.

Corporate practice of medicine laws remain a major hurdle

While many of the above-described transactions offer distinct advantages (including expanded geographic reach and market share, greater efficiencies and economies of scale, synergies with current private equity holdings, and access to management expertise), they risk violations of state corporate practice of medicine prohibitions.

Generally speaking, state corporate practice of medicine prohibitions restrict corporations from practising medicine or employing physicians to provide professional medical services. Although these regulations vary significantly across the 33 states that currently have such prohibitions, they are generally designed to prevent the commercialisation of the practice of medicine, avoid conflicts of interest between a corporation's obligations to its shareholders and physicians' obligations to their patients, and eliminate any interference with a physician's medical judgement.

By their very nature, telemedicine and digital health typically transcend jurisdictional boundaries. As result, compliance with ownership, employment and other obligations in one state may not ensure compliance in another. This diversity of rules and exceptions has the effect of limiting the formation, development and use of telemedicine alternatives for fear of creating legal exposure, particularly when the very entities most likely to have the resources and scale to provide effective telemedicine are often corporations.

Typically, attempts to tighten corporate practice of medicine laws have come from within state legislative bodies, while enforcement of these laws has been the focus of state attorneys general. However, recent court cases – including the American Academy of Emergency Medicine Physician (AAEMP) Group lawsuit filed in December 2022 against Envision Healthcare – may offer a view of things to come. In the suit, AAEMP (backed by the California Medical Association) alleges that Envision is using "shell business structures" in order to circumvent California state corporate practice of medicine regulations and improperly allow it to maintain ownership (or effective control) of emergency department staffing groups. Although still in its early stages, the litigation is worth watching, as it may encourage other private parties to use state corporate practice of medicine laws as a means of winning business disputes.

In any case, until such time as state legislatures take into account new methods for delivering care – and the financial and operational arrangements that support such methods – telemedicine providers and healthcare entities that contract with providers will need to scrutinise their contracts and structures on a state-by-state basis to avoid running up against state corporate practice of medicine prohibitions.

Regulatory scrutiny of telehealth fraud and over-utilisation gains strength

In September 2022, the HSS Office of the Inspector General (HHS-OIG) issued a data brief that identified Medicare provider billing practices that it was concerned posed a high risk to programme integrity. Subsequently, in April 2023, HHS-OIG issued a new toolkit that would enable

public and private entities, private health plans, state Medicaid fraud control units and federal healthcare agencies to conduct compliance assessments and self-assessments that could identify potential healthcare programme risks.

In its overview of the toolkit, OIG noted that telehealth services are "now an important part of our healthcare system", and pointed to the fact that Medicare beneficiaries used 88 times more telehealth services during the first year of the COVID-19 pandemic than in the previous year. The toolkit is designed to provide stakeholders and policymakers with a better understanding of the programme integrity risks associated with telehealth services and to help them develop necessary safeguards and address individual cases of potential fraud, waste and abuse.

The toolkit consists of two components:

- tools for identifying and analysing telehealth claims data; and
- a set of seven programme integrity measures that use the gathered data to determine the existence of potential risks.

Coupled with an uptick in law enforcement actions, OIG's series of initiatives makes it clear that, in some cases, fears of fraud and abuse from a minority of telemedicine practitioners have been realised. That said, despite increased use of telemedicine services, there appears to be no clear evidence that this method of care delivery gives rise to higher rates of fraudulent or inappropriate activity compared to other care delivery methodologies. If anything, the investigations conducted and charges filed throughout the past several years indicate that, when applied, fraud and abuse laws are strong and that payers will – and should – continue to scrutinise programmes regardless of source or focus.

Dobbs decision shines a spotlight on reproductive telehealth

No review of the state of digital health in 2023 in the United States can fail to take note of the widespread impact of the US Supreme Court's landmark June 2022 ruling in Dobbs v Jackson Women's Health Organization. In reversing its prior decisions in Roe v Wade and Planned Parenthood of Southeastern Pennsylvania v Casey, the Court stated that the US Constitution does not confer a right to abortion and returned the authority to regulate abortion "to the people and their elected representatives". In lieu of congressional action at the federal level, the Dobbs decision has essentially created a state-level system of access (or not) to abortion and many other reproductive health services.

In the eyes of many, the decision has also created chaos.

The choice of having or performing an abortion is an extraordinarily complex decision, and few areas of healthcare practice and regulation give rise to as much debate in this country. Although opinions on the subject vary from one extreme to another and include a vast middle ground, there is one point of almost universal consensus: Dobbs has had an unprecedented impact on the ability of individuals to obtain – and physicians and nurses to provide – effective, comprehensive maternal and reproductive healthcare without fear of legal, financial or reputational ruin.

While the purpose of this section is not to take a deep dive into the moral, political and other arguments in favour of or against abortion (or even propose a balanced approach that attempts to resolve the numerous concerns surrounding the issue), it must be noted that telemedicine and digital health solutions are at the centre of many

of the discussions, state-level legislative debates and federal regulatory actions occurring today.

In the wake of Dobbs, a number of states quickly passed laws restricting access to abortion or had existing laws against abortion that came into effect immediately following the Supreme Court's decision. Many of these laws had significant, unintended consequences, particularly for patients needing – and physicians performing – lifesaving medical procedures.

At the same time, many other states have actively expanded access to abortion treatment and enshrined protections into law for in-state and out-of-state individuals providing or seeking medical treatment within their jurisdictions.

For individuals and practitioners caught between conflicting state laws, telehealth solutions are providing a notable option. Since the onset of the COVID-19 pandemic and following the Dobbs decision, there has been a surge in demand for telehealth medical abortion services. According to a December 2022 update by the Guttmacher Institute, medication-based abortions accounted for more than half of all abortions in the United States, and one fifth of these procedures occurred via telehealth.

As the time of writing (spring 2023), US states are split almost evenly when it comes to legal telehealth medication abortions, with two dozen states and the District of Columbia allowing the procedure, and slightly less than half of states either expressly or in effect banning this form of medical treatment.

The courts are also split with regard to the legality of the primary drug used for telehealth medication abortions: mifepristone. In January 2023, among other actions, the US Food & Drug Administration (FDA) lifted restrictions that prevented patients from obtaining medication abortion pills from retail pharmacies in states that do not have bans against medication abortions. In the meantime, lawsuits in Texas and Washington state (seeking to, respectively, reverse FDA approval of mifepristone and force the FDA to make no changes to the availability of the medication) were working their way through the federal district and appellate courts.

On 21 April 2023, the Supreme Court weighed in, blocking the decision of the US Court of Appeals for the Fifth Circuit to allow limited implementation of the Texas court's earlier decision to fully ban the use of mifepristone. While the Supreme Court's decision means that the drug will be widely available in those states where abortion is legal for up to ten weeks in a pregnancy, it does little to resolve the ongoing debate regarding abortion and, in particular, the use of telehealth to provide abortion and reproductive services.

Given the current, divided federal government, it is unlikely that abortion-related reproductive health legislation of any sort will be passed anytime soon, leaving millions of patients and practitioners with extremely difficult choices.

Shifting away from the abortion debate, however, states on all sides of the political divide have also begun taking action that would improve maternal care to expectant mothers via telehealth. Georgia, for example, recently enacted SB 106, known as the Healthy Babies Act. As part of an effort to increase state Medicaid benefits for at-risk mothers in underserved rural communities, the legislation creates a three-year pilot programme, beginning in FY 2024, for remote maternal health services through the state's Department of Community Health.

In New York, progress has been made on legislation (A 3004) that aims to provide funding for regional perinatal care centres and other health providers to launch telehealth applications. These and similar initiatives in other states indicate strong support for the provision of maternal healthcare services via telemedicine.

Patient data privacy and cybersecurity are ongoing concerns

Like all healthcare professionals, telemedicine providers in the United States are subject to HIPAA and the HITECH Act, as well as a range of more recent federal and state data privacy and breach notification laws, such as the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act. Such laws have been established because healthcare data and personally identifiable information are rich targets for hackers and cyber criminals.

According to data provided by the HHS-OIG, in 2022 there were 707 reported healthcare data breaches involving more than 500 records each – down just slightly from 2021's record-setting 715 reported healthcare data breaches of a similar size, and nearly double the amount reported in 2018. The majority of these 2022 breaches were incurred by healthcare providers (compared to health plans or business associates).

Despite these risks, wider exposure to telemedicine has led to rapid acceptance among patients, providers and insurers – a degree of enthusiasm that should be encouraged while also advocating for more stringent health IT security standards. Providers should ensure that they seek out and retain the services of reputable vendors that provide full interoperability with existing electronic medical record systems, are willing to sign business associate agreements, and provide reliable customer service while maintaining robust data security measures.

Telemedicine providers will also need to establish and document clear guidelines about what types of patient information can be collected and how such data can be disseminated and used to guide care. Patients are in a uniquely vulnerable position when working with providers, particularly those patients whose mental and physical health issues may impair their ability to understand fully or agree to the terms of a telemedicine visit.

Conclusion

Telemedicine has gained wider acceptance among patients, providers, hospitals and insurers. Although the rollback of some pandemic-related waivers is likely to continue, increased pressure on lawmakers and regulators will likely act as a counterweight, encouraging the implementation of laws and policies that will enable digital health services to reach their full potential. To achieve this potential, however, digital health services will need to overcome a number of persistent barriers.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com