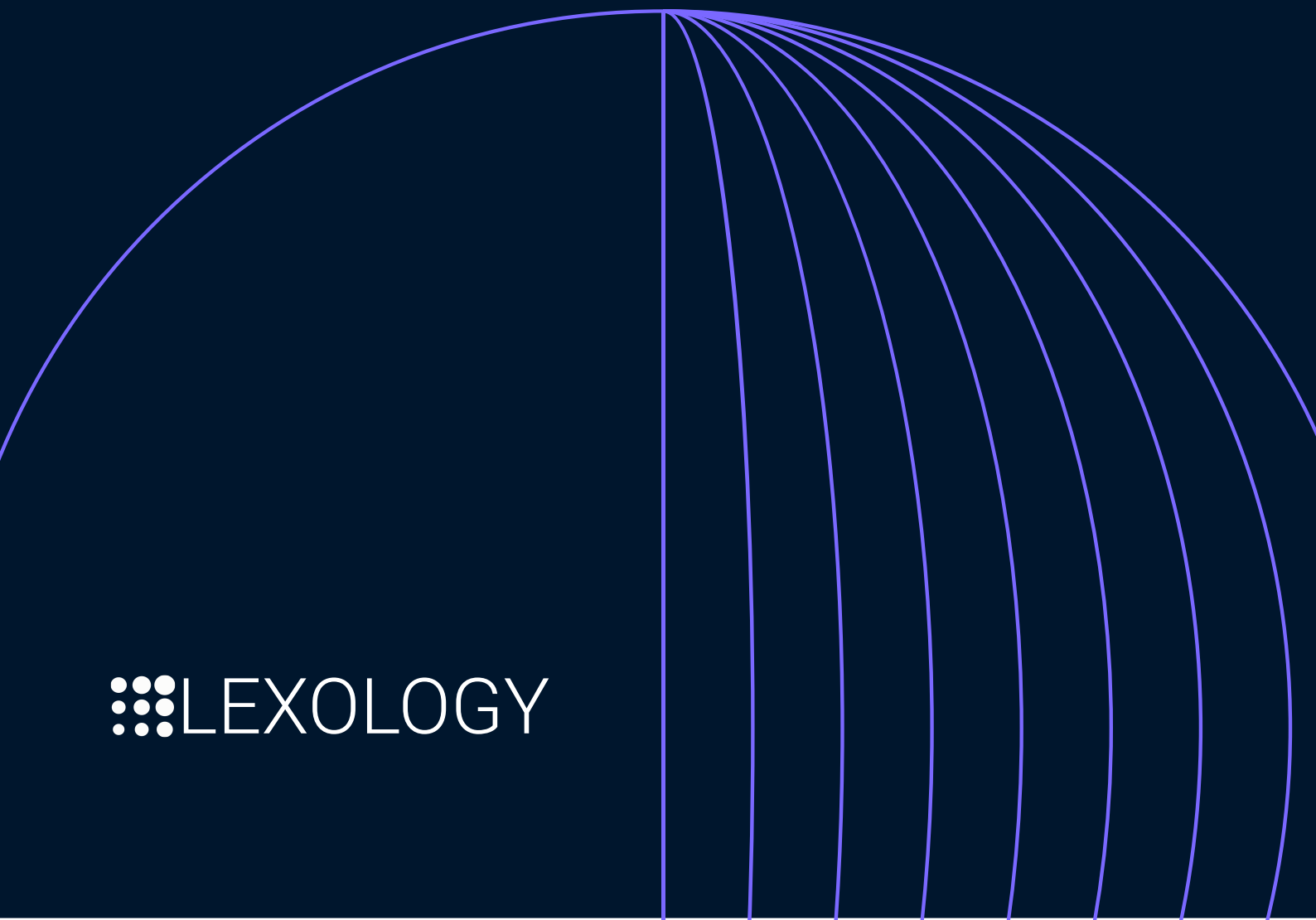
PANORAMIC

DIGITAL HEALTH 2024

Contributing Editor

Abeba Habtemariam

Arnold & Porter



LEXOLOGY

Digital Health 2024

Contributing Editor

Abeba Habtemariam

Arnold & Porter

Quick reference guide enabling side-by-side comparison of local insights, including market overview; legal and regulatory framework; data protection and management; intellectual property rights, licensing and enforcement; advertising, marketing and e-commerce; payment and reimbursement; and recent trends.

Generated on: March 21, 2024

Contents

Thailand

Peerapan Tungsuwan, Nont Horayangura, Panyavith Preechabhan, Praween Chantanakomes

Baker McKenzie

USA

Abeba Habtemariam, Nancy L Perkins, Chris Anderson, Monique Nolan, Alice Ho

Arnold & Porter

Australia

Susan Jones, **John Lee** , **Andrew Hii**
Gilbert + Tobin

Summary

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

Key players include:

- the Australian Government, which has provided for A$106.5 billion for health in the 2023–24 budget, which represents 15.6 per cent of the Australian Government's total expenditure. The Federal Government funds health services through the Department of Health and Aged Care (DoHAC), the Therapeutic Goods Administration (TGA), the Medical Research Future Fund (MRFF) and the Australian Digital Health Agency (ADHA), which is responsible for the National Digital Health Strategy and Framework for Action and operates My Health Record, an online platform that aggregates an individual's key health information and provides interoperability between clinical information systems across the health sector;
- state and territory governments, which, among other things, operate Australia's public hospitals, including emergency departments and ambulance services;
- private healthcare businesses, including operators of private hospitals, day surgeries, primary and referred care clinics and imaging and pathology services;
- healthcare professionals;
- developers and suppliers of digital health systems;
- private health insurers;
- venture capital and private equity funds;
- academic institutions, especially the Commonwealth Scientific and Industrial Research Organisation and universities;
- a range of cross-sector innovation and commercialisation bodies, including ANDHealth, the Digital Health Cooperative Research Centre and MTPConnect; and
- industry associations, including the Medical Software Industry Association, the Medical Technology Association of Australia, AusBiotech, BioMelbourne Network and the Australasian Institute of Digital Health.

Participants in the healthcare industry (government and private) are increasing their adoption of digital health technologies in order to improve health outcomes, meet the needs of their stakeholders and respond to various health system issues (eg, increasing rates of chronic conditions, emphasis on prevention, management and in-home care, focus on value-based healthcare, declines in private health insurance, crisis in aged care, inequality in access to health services, hospital waiting times and budget pressures). Key areas of focus include telehealth and virtual health services (including for mental health and aged care), AI, interoperability, health informatics, payments and e-referral and booking.

Law stated - 25 January 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

Over the past decade, the private health sector has led the developments in the digital health industry. However, federal, state and territory government-funded investments have significantly increased over the past few years. The covid-19 pandemic, the 2019–2020 bushfires, the Royal Commission into Aged Care Quality and Safety and the Productivity Commission's report into Mental Health have all accelerated investment in digital health and greater coordination between governments and private sector participants. The Australian Government estimates that it delivered 10 years of reform in 10 days with the 2020 introduction of whole-of-population access to telehealth under Medicare.

The pandemic-driven focus on the need to shift patients out of physical sites, unless totally necessary, has created a more agile and responsive Australian healthcare system, and this shift requires ongoing investment into the development and implementation of new technologies. ANDHealth, one of Australia's leading health technology commercialisation organisations, reported in its FY2023 Industry Sentiment Survey – Commercialising Digital Health in Australia – that a lack of digital health specialised investors and limited access to capital remain the most significant impediments to commercialising new health technologies in Australia.

However, the key challenge in the Australian digital health industry remains funding and access to capital to drive commercialisation of innovations. This has been particularly relevant in respect of foreign investment following temporary restrictions that were implemented in the Australian foreign investment regime in response to the covid-19 pandemic. Although many of these restrictions were lifted on 1 January 2021, foreign investment continues to be a key regulatory hurdle, particularly in relation to digital health investments with material technology or data assets.

Lack of reimbursement also remains another significant challenge for investment in digital health. Broader reimbursement of telehealth as a model of care and a clear regulatory landscape for Software as a Medical Device products are a large step forward for the growth of Australia's domestic digital health industry. However, there are many other types of solutions in the sector that currently have no defined or well-understood reimbursement pathway. Industry has identified current non-specific healthcare reimbursement policies as a substantial barrier to commercialisation and implementation of digital health technologies, specifically in the areas of digital medicine and digital therapeutics.

Law stated - 25 January 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

In the private sector:

- In December 2023, Medibank Private secured a binding deal to become the controlling shareholder in GP clinics chain MyHealth. Medibank acquired an additional 41 per cent stake in Myhealth Medical Holdings Pty Ltd for A$51.81 million.
- In August 2023, allied healthcare organisation Healthia received a buy-out proposal from Harold BidCo for 100 per cent of its fully diluted share capital, with the acquisition valued at A$227 million.
- In March 2023, HMC Capital signed an A$1.2 billion deal to acquire a portfolio of private hospitals owned by US investor Medical Properties Trust.
- In September 2022, ASX-listed company Advanced Human Imaging Ltd announced it had entered into an arrangement agreement to acquire all outstanding shares of Canadian company wellteq Digital Health Inc. The shareholders of wellteq Digital Health Inc and the Supreme Court of British Columbia approved the plan of arrangement in November 2022 and completion occurred in early December 2022.
- In September 2022, Pfizer acquired ASX-listed, University of Queensland startup ResApp Health Limited for A$179 million. ResApp Health Limited has developed smartphone technology to diagnose and measure the severity of respiratory diseases based on analysis of a patient's cough.
- In August 2022, biotech investor Dr Glenn Haifer and Ampersand Capital Partners, a global healthcare private equity firm, acquired AcuraBio (formerly Luina Bio), a leading Australian biopharmaceutical contract development and manufacturing company (CDMO), for an undisclosed amount.
- In August 2022, private equity firm Adamantem Capital acquired 100% of the share capital in GenesisCare's cardiology businesses - Genesis Heart Care Pty Ltd and Genesis Sleep Care Pty Ltd – for between A$200 million and A$250 million.
- In July 2022, private equity firm Pemba Capital Partners acquired the group of companies operating as SACARE, a leading South Australian operator of supported accommodation and care services for people living with a complex disability, for an undisclosed amount.
- In July 2022, equity firm BGH Capital completed its successful off-market cash takeover of IVF provider Virtus Health for A$697 million.
- In April 2022, Cochlear announced its intention to acquire hearing solutions provider Oticon Medical for approximately A$170 million. On 1 December 2022, the Australian Competition and Consumer Commission (ACCC) announced it has significant preliminary competition concerns in relation to the proposed acquisition. The ACCC's provisional date for announcement of its decision is 16 March 2023.
- In January 2022, bioanalytical laboratory business Agilex Biolabs was acquired by Australian healthcare company Healius for an enterprise value of A$301.3 million.

In the public sector:

- The A$101 billion committed to health by the Australian Government in the 2023–24 budget included investments to build a stronger Medicare (A$5.7 billion), health prevention and protection (A$1.1 billion), tackling smoking and vaping ($737.0

million), mental health and suicide prevention (A$586.9 million), and First Nations health (A$818.5 million).

- In March 2022, the Australian Government announced an investment of A$107.2 million to modernise the Australian healthcare system. This includes A$72 million towards the transformation of health payments and services, A$32.3 million towards the 2018–2022Intergovernmental Agreement on National Digital Health (IGA) and A$2.9 million towards the Australian Institute of Health and Welfare (AIHW) to safeguard national health data.

Law stated - 25 January 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

Key issues in due diligence include:

- understanding how the company complies with Australian privacy and data regulations (which are particularly important for healthcare companies given the sensitivity of the information being handled), including protecting data assets and flows critical to the company's operation; and
- ensuring that a company has necessary ownership or rights to use information technology that is key to the business, including necessary rights to license its products commercially.

Specifically, we recommend addressing the following due diligence issues:

- Privacy: ascertain whether a company's privacy policies provided to customers upon collection of personal information are compliant with the Privacy Act 1988 (Cth) (the Privacy Act) and the Australian Privacy Principles (APPs). Specifically, consider compliance with requirements regarding obtaining consent for collection of sensitive information (which includes health information). We note that the Australian Government is currently reviewing the Privacy Act, and that these reforms are expected to increase the privacy protections afforded to individuals.
- Data: report on the types of data (including personal information and sensitive information) collected and held by the company and how this data and personal information is obtained and used by the company, to ensure compliance with the APPs. Report on any transfers of personal information or data-sharing relationships, including any arrangements for the outsourcing of data-processing activities and any disclosure of data and personal information overseas, to ensure compliance with APP 8.
- Cybersecurity: report on any information security or cyber incidents, regulatory investigations and complaints regarding the company's privacy handling or marketing activities that have taken place in the past five years, as well as undertaking an assessment of a company's cybersecurity measures and whether

the company has policies and procedures in place to respond to any cybersecurity incident or breach. Assess whether the company is subject to the recently amended Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) (which captures certain entities in the healthcare and medical sector) and if so, review the company's preparedness with respect to compliance with the SOCI Act, for example, identification of relevant assets, development of risk management and incident notification plans (eg, 'Critical Infrastructure Risk Management Program'), review and amendment of material contracts to address compliance obligations (eg, to address the Government's rights to require access to information, or to give directions or exercise step-in rights).

- Ownership of key IT systems: review any material IT agreements (including software licensing agreements) entered into by the company. Report on the key information technology (including any products, hardware and software) or third-party services used by the company to assess whether it has ownership of or right to use such information technology.

Law stated - 25 January 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

There are no financing structures that are unique to digital health ventures in Australia; financing structures are determined largely based on more typical considerations regarding the financial profile of the relevant target (for example, what stage the relevant target is at in its life cycle).

In December 2023, the DoHAC published its Digital Health Blueprint for 2023-2033 (Blueprint). The Blueprint establishes a key focus and coordinated path to ensure that the Australian health system can 'safely and securely' use health data to inform health system planning and new treatments and therapies, to encourage innovation and ensure Australia's health system can respond to emerging technologies as they are developed. The Blueprint is accompanied by an Action Plan that outlines the Albanese Government's A$950 million investment (over four years) in digital health, as well as its mid-term goals (2025–2028) and long-term goals (2028 onwards). The Action Plan outlines the following initiatives and investments to be undertaken:

- progressing national digital health reforms, including investment by the Government of A$325.7 million over four years from 2023–24, to establish the ADHA as an ongoing entity;
- the introduction of My Medicare as a new voluntary system for patients and healthcare providers to support better care for people who choose to register with their general practice and nominate their usual GP (partnering with healthcare providers and organisations, the ADHA and Services Australia);
-

ongoing health policy efforts (including working with international partners and key bodies such as the Global Digital Health Partnership, and the World Health Organization);

- modernisation of My Health Record (partnering with the ADHA), including the Australian Government's investment of A$38.4 million over two years from 2023–24 to commence the transition of My Health Record from being a clinical document (PDF) system to an atomic data-rich platform;
- enhancing My Health Record capabilities, including the Government's allocation of A$13.1 million over two years from 2023–24, to enable default sharing of key health information with My Health Record, and its investment of A$5.8 million over two years starting in 2023–24 to support allied health software vendors in connecting to My Health Record;
- enhancing medication management, including the Government's investment of A$111.8 million over four years from 2023–24 to deliver a stable and sustainable electronic prescription delivery service, as well as the mandatory use of electronic prescriptions for high-risk and high-cost medicines;
- national standards to support health system interoperability, including continued investment in the Health Delivery Modernisation (HDM) Program, modernising the Healthcare Identifiers legislative framework as part of the HDM Program, investing A$9.3 million over two years from 2023–24 for the CSIRO to work with all Australian governments, the ADHA and the health technology industry to establish a core national standard for consistent patient health interaction information capture through community consensus, and investing A$5.8 million over two years from 2023-24 for the DoHAC to collaborate with key sector stakeholders to design a national eRequesting capability;
- national health information exchange capabilities, including development of a National Health Information Exchange Architecture and Roadmap under the IGA, and, as part of the 2023–2024 Budget, the Department's investment to support the states and territories to undertake preliminary legislative policy and analysis work to identify options to develop a national legislative framework authorising national health information sharing across care settings and borders;
- workforce development initiatives, including expanding upon the Capability Action Plan, which aims to equip Australia's health workforce for a digitally enabled future, as co-funded in part by the Government through the IGA, including creating an online hub for digital career pathways for clinical and non-clinical professionals (partnering through the AIDH and the ADHA);
- various mental health initiatives, including the Initial Assessment and Referral (IAR) Guidance and the IAR-Decision Support tool, designed to provide a consistent approach for clinicians to confirm the level of mental health care a patient requires;
- digital initiatives supporting population health, such as the Cardiovascular Disease (CVD) Risk Guideline and calculator to manage CVD risk. In the 2023–2024 Budget, the Government committed A$1 million to commence implementation of the new guideline and embedding of the calculator into GP software;
- genomics initiatives, including the Government's consultation with states and territories, through the Health Technology and Genomics Collaboration, on the

establishment, design, and remit of a new national genomics body, as well as the provision of funding for genomics research through the Genomics Health Future Mission of the MRFF, which was valued at A$21.969 billion in September 2023; and

- aged care initiatives, including 'Support at Home Assistive Technology', 24/7 registered nurses coverage and the publishing of financial data items of residential aged care providers on My Aged Care by 'Dollars Going to Care' (alongside 'Care Minutes' and 'Star Ratings').

The Action Plan also points to national investments into artificial intelligence (AI) technologies, for example:

- the National Artificial Intelligence Centre, which will help drive adoption and use of transformative AI technologies, by managing Australia's AI expertise and address barriers to small and medium-sized enterprises adopting and developing AI and emerging technology; and
- the TGA, which is working with other major regulatory agencies in the International Medical Device Regulators Forum to establish an optimal regulatory approach for AI-enabled medical devices.

Other Australian Government initiatives include:

- the Digital Restart Fund that supports digital and information and communications technology (ICT) initiatives across the Government sector;
- in January 2023, the South Australian government approving A$31 million to extend the rollout of the Sunrise electronic medical record and patient administration system to the state's regional local health networks;
- the Digital Health Cooperative Research Centre operates through collaborative R&D programmes between government, industry and academia to foster new companies and products, a new digital health workforce and forge new national and international partnerships;
- the R&D tax incentive provides a tax offset for eligible R&D activities. It has two core components: a refundable tax offset for certain eligible entities whose aggregated turnover is less than A$20 million and a non-refundable tax offset for all other eligible entities; and
- the Early Stage Venture Capital Limited Partnership programme helps fund managers attract pooled capital so they can raise new venture capital funds of between A$10 million and A$200 million to invest in innovative Australian early-stage businesses, offers tax benefits to fund managers and investors and connects investors with early-stage businesses.

Law stated - 25 January 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 | What principal legislation governs the digital health sector in your jurisdiction?

The legislation that governs competition in the digital health sector is the Competition and Consumer Act 2010 (Cth) (CCA), which is the standard competition law framework in Australia. The CCA also includes the Australian Consumer Law (ACL), which covers consumer protection issues. There are no special rules for the digital health sector.

Additional key legislation includes the Therapeutic Goods Act 1989 (Cth) (TGA Act), which regulates all therapeutic goods, that is medical devices, medicines (including complementary, over-the-counter and prescription), the Therapeutic Goods Regulations 1990 (Cth), and the Therapeutic Goods (Medical Devices) Regulations 2002 (Cth) (together, the TGA Regulations). The TGA Act was updated in 2021 to address the increase in medical-related software-based products being developed. The TGA Act includes new classification rules for software-based medical devices, including for those that provide a diagnosis for health conditions, monitor the state of health conditions, specify a treatment or provide therapy. The reforms also amend the 'Essential Principles' – the requirements relating to the safety and performance of medical devices – in relation to cybersecurity, the management of data and information, and requirements relating to development, product and maintenance of medical devices. These changes have brought Australia's approach into alignment with those of our key trading partners.

Digital health technologies that collect personal information will also need to comply with Australia's privacy laws as set out in the Privacy Act. As health information is highly sensitive personal information, the Privacy Act includes more robust protections around its collection and handling by all organisations that provide a health service and hold health information. The Office of the Australian Information Commissioner (OAIC) also regulates the treatment of health information contained in individuals' health records (My Health Record) and healthcare identifiers operated by Medicare. The operation of the My Health Record scheme is governed by the My Health Records Act 2012 (Cth).

Law stated - 25 January 2024

Regulatory and enforcement bodies

7 | Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

The Australian Competition and Consumer Commission (ACCC) enforces the CCA in Australia. The ACCC has a Digital Platforms Branch responsible for the ACCC's ongoing scrutiny of digital platform markets. Although the ACCC's investigations and inquiries into digital platforms are not specifically focused on the digital health sector, the outcomes of the ACCC's enforcement and regulatory actions do have implications for digital health businesses.

The TGA regulates medical devices, including Software as a Medical Device, such as software that uses information about symptoms to make a diagnosis, and mobile apps coupled with devices for calculating medication dosages.

The OAIC enforces compliance with the Privacy Act and other privacy laws, in particular to ensure the proper handling of personal information, including regulating the treatment of health information contained in individuals' health records (My Health Record) and healthcare identifiers operated by Medicare.

In June 2022, the Australian Government formed the Digital Platform Regulators Forum (DP-REG), which comprises the ACCC, the OAIC, the Office of the eSafety Commissioner and the Australian Communications and Media Authority (ACMA). DP-REG is an avenue for the independent Australian regulators to share information about and collaborate on digital platform regulation with a view to strengthening whole-of-government responses to key issues. The DP-REG is not a decision-making body and has no bearing on its members' existing regulatory powers, legislative functions or responsibilities. In September 2023, the members of DP-REG set out how they are working together to understand the new opportunities and challenges presented by AI and how existing regulatory frameworks might apply to AI in a joint submission to the Department of Industry, Science and Resources consultation on its 'Safe and responsible AI in Australia' Discussion Paper published in June 2023.

The ACMA is also likely to become a more prominent regulator in digital health, after its June 2023 report on digital platforms' efforts under the Australian Code of Practice on Disinformation and Misinformation. ACMA's report found that there is growing concern in Australia about disinformation and misinformation, particularly in the context of events such as the Russian invasion of Ukraine and various elections. On 25 June 2023, the Australian Government released the draft Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 for public consultation.

Law stated - 25 January 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

Generally, therapeutic goods, including digital medical devices, need to be registered on the Australian Register of Therapeutic Goods (ARTG) prior to being sold in Australia. For example, software that meets the definition of a 'medical device' under the TGA Act needs to be registered on the ARTG before it can be supplied. Accordingly, the impact of regulation under the TGA Act should be considered by inventors in the early stages of product development.

Law stated - 25 January 2024

Soft law and guidance

9 Is there any notable 'soft' law or guidance governing digital health?

In Australia, there are no guidelines on the application of competition law specific to digital health markets. The ACCC's approach to competition law generally is reflected in various guidelines including its merger guidelines and authorisation guidelines (merger and non-merger), misuse of market power guidelines and concerted practices guidelines.

The ACCC (together with state and territory consumer protection agencies) has also developed several practical guidelines on consumer protection issues such as unfair business practices, consumer guarantees, consumer product safety and sales practices.

The Australian Digital Health Agency (ADHA) is responsible for the development and operation of a national digital health strategy, as well as development and implementation of specifications and standards in relation to digital health. Additionally, the ADHA has developed a Cyber Security Strategy for 2022-2025, which aims to uplift capability within the ADHA in response to the changing cyber environment. The ADHA publishes guides and other resources that may be relevant to providers of digital health products and services. The ADHA has also recently introduced its National Healthcare Interoperability Plan for 2023-2028, which identifies 44 actions to be taken to share consumer health information and data in a 'safe, secure and seamless manner'. The actions stretch across five priority areas related to identity, standards, information sharing, innovation and measuring benefits.

The TGA provides guidance in relation to the regulation of software-based medical devices to assist manufacturers and sponsors to understand the TGA Act's regulation of such devices (see Regulation of software based medical devices). It also provides guidance for patients and consumers, among others, to inform them about the potential cybersecurity risks that may arise with connected medical devices (see Medical device cyber security information for users - Guidance for patients and consumers).

Law stated - 25 January 2024

Liability regimes

10 What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

In consumer protection, the ACL applies to digital health goods and services, including as follows:

- it prohibits misleading or deceptive conduct and false or misleading representations made in the course of advertising goods or services. The value of a penalty unit increased in July 2023 from A$275 to A$313 (for infringement notice penalties), and the maximum penalty for making a false or misleading statement was substantially increased in October 2022 and is now the greater of:
    - A$50 million;
    - if the Court can determine the value of the 'reasonably attributable' benefit obtained from the breach, three times that value; or

  - if the Court cannot determine that value, 30 per cent of adjusted turnover over the period that the breach occurred (which is a minimum period of 12 months);

- it grants automatic quality guarantees to consumers of goods or services. It also requires suppliers (and in some cases manufacturers) to remedy a failure to comply with the guarantees and to compensate consumers for reasonably foreseeable loss caused by the failure;
- it also enables plaintiffs to recover losses from manufacturers that supply products with safety defects;
- it sets out an 'unfair contract terms' regime that governs terms contained in standard-form consumer or small business contracts. In October 2022, Parliament passed the Treasury Laws Amendment (More Competition, Better Prices) Bill 2022 (Cth), which made unfair contract terms unlawful and subject to civil penalties from 9 November 2023;
- consumers may bring actions for misleading or deceptive conduct, consumer guarantee failures or product safety breaches as a class.

In the context of the TGA Act, to be able to import and supply a medical device in Australia, the medical device is required to meet the Essential Principles for safety and performance. Failure to meet the Essential Principles can result in civil or criminal penalties under the TGA Act. The Essential Principles require the minimisation of risks associated with the design, long-term safety and use of the device, which implicitly includes minimisation of cybersecurity risks.

Law stated - 25 January 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 | What constitutes 'health data'? Is there a definition of 'anonymised' health data?

Health data includes:

- information or an opinion about an individual's health or any health services provided, or to be provided, to the individual;
- any personal information collected to provide or in providing a 'health service' to an individual (including organ donation); and
- genetic information about an individual that is in a form that could be predictive about the health of an individual (or relative of the individual).

The concept of 'providing health services' is very broad and can capture a range of services that may not be front of mind when thinking about health – for example, information collected by a gym on an individual in connection with a gym class, or Medicare billing information held by an insurance provider or debt collector.

Anonymised health data is not defined, although the Australian Privacy Principles (APP) Guidelines state that 'anonymity' means that an individual dealing with an entity cannot be identified. Critically, health data that may be anonymous in the hands of one entity may not be anonymous in the hands of another. The ability of an entity to link a data set with other information is relevant to whether data is truly anonymised.

Law stated - 25 January 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Given the sensitivity of health information, its collection, use and management is regulated by the Privacy Act.

Health data is treated more strictly than personal information under the Privacy Act. Health data is a subset of 'sensitive information' and consent is required for its collection.

Generally, an organisation can collect health data from a person if:

- the person provides their consent (express or implied); and
- the information is reasonably necessary for the organisation's activities.

Implied consent arises when consent can be inferred from the circumstances and conduct of the person providing the health information. This is a higher test than that imposed on other personal information. The Australian Government is currently undertaking a review of the Privacy Act. As part of this review, the Government is considering updating the definition of 'consent' to be voluntary, informed, current, specific and an unambiguous indication through clear action.

APP 11 requires entities to take reasonable steps to protect personal information (including sensitive information, such as health information) it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. According to the Office of the Australian Information Commissioner (OAIC)'s APP Guidelines, 'reasonable steps' will depend on the circumstances in each particular case and may include governance, culture and training, internal practices, procedures and systems, ICT security, access security, and destruction and de-identification.

In addition, the handling of health information is also subject to certain state-based legislation, which differs from the Privacy Act in some aspects, but the differences are relatively minor. Recently, the Attorney General's Privacy Act Review Report, released on 16 February 2023 (Attorney General's Report), noted that harmonisation between health privacy legislation may have the greatest benefit to individuals due to the risk of harm and discrimination if health information is disclosed without authorisation. The Report noted that proposed focus areas included the classification of genomic information, coverage of the deceased, and the interaction between genomic information and deceased individuals or at-risk relatives. The Report further noted that the Commonwealth, state and territory governments are undergoing a consultation process about access to social

media accounts and digital records upon death or incapacity. In its response to the Attorney General's Report, published on 28 September 2023 (Government's Privacy Response), the Government agreed in principle to the Attorney General's proposal to establish a Commonwealth, state and territory working group to harmonise privacy laws.

Law stated - 25 January 2024

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

APP 2 provides that individuals must have the option of dealing anonymously or by pseudonym with entities subject to the Privacy Act. However, entities are not required to provide these options if the entity is required or authorised by law to deal with identified individuals or it is impracticable for the entity to deal with individuals who have not identified themselves. There may also be practical consequences for patients who do not wish to identify themselves, as their ongoing healthcare may be difficult for organisations to manage and they are unlikely to be able to claim a Medicare or health fund rebate.

De-identification may be one way to protect the privacy of individuals. De-identification involves removing personal identifiers (such as name, address, date of birth, etc) and removing or altering other information that could identify an individual (such as unique characteristics). However, with the increasing capability of technology and the sophistication of cyber attacks, it is becoming more and more difficult to de-identify data effectively. The Australian Government is currently reviewing the Privacy Act, and considering increasing the relevant threshold from 'de-identified' to 'anonymous' (for information to no longer be considered 'personal information').

Types of de-identified health data include Medicare numbers and healthcare identifiers. Medicare numbers are primarily used by individuals to claim benefits under the Medicare Benefits Scheme. APP 9 restricts the use or disclosure of a patient's Government-related identifier to specific circumstances (eg, it is reasonably necessary to verify the patient's identity for an organisation's activities).

Healthcare identifiers are unique 16-digit numbers that identify individual healthcare providers, healthcare provider organisations (such as digital health organisations) and individuals receiving healthcare. Healthcare identifiers help to reduce the potential for mix-ups with health data and are the foundation for Government initiatives such as the My Health Record system, in which individuals' health information can be viewed securely online. They are not health records, but are limited to identifying information such as name, date of birth and sex to uniquely identify patients. Use of healthcare identifiers is regulated by the Healthcare Identifiers Act 2010 (Cth) and Healthcare Identifiers Regulations 2020 (Cth), which provide that healthcare identifiers may only be collected, accessed, used and disclosed for limited purposes (such as providing healthcare, for example, by using it to access the My Health Record of a healthcare recipient). In circumstances where a healthcare identifier is used or disclosed for purposes not permitted by the legislation, criminal and civil penalties may apply.

The Attorney General's Report proposed that the protections under APP 11 (Security of Personal Information) should be extended to de-identified information, so that entities are required to take steps as are reasonable in the circumstances to protect de-identified information:

- from misuse, interference and loss; and
- from unauthorised re-identification, access, modification or disclosure.

The Attorney General's Report similarly proposed that protections provided to personal information under APP 8 (overseas disclosure) should be extended to protect de-identified information, including ensuring that the entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.

The Government stated in the Government's Privacy Response that it generally agrees with the intent of protecting de-identified information from unauthorised re-identification and will consider further how this objective may be able to be achieved.

Law stated - 25 January 2024

Enforcement

14 How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The Privacy Act gives the Privacy Commissioner a range of privacy regulatory powers, including powers that allow the OAIC to work with entities to facilitate best privacy practices, as well as investigative and enforcement powers to use in response to privacy breaches.

For example, if a healthcare company fails to obtain consent to collect the health information of an individual, the company will be in breach of APP 3 regarding the collection of sensitive information.

A breach of an APP is an 'interference with the privacy of an individual' under section 13(1) of the Privacy Act and, although it is not a civil penalty provision, it can lead to regulatory action and penalties. The provisions of the Privacy Act are enforceable under Parts 6 and 7 of the Regulatory Powers (Standard Provisions) Act 2014 (Cth), which provide for enforceable undertakings and injunctions to be issued to enforce provisions.

In March 2019, the Australian Government first announced its intention to investigate the effectiveness of Australia's current data protection regime and reform the Privacy Act, including by introducing higher penalties for breaches of the Privacy Act. In November 2022, the first legislation tabled in Australian Parliament in connection with this review – the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Privacy Bill) – passed both Houses of Parliament. The Privacy Bill covers four key objectives with respect to the Privacy Act:

-

to significantly increase the maximum penalty for serious or repeated interferences with the privacy of an individual under the Privacy Act, increasing the former penalty from A$2.22 million (for corporate entities) to the greater of A$50 million, three times the value of any benefit directly or indirectly obtained from the contravention, or, if the value of the benefit cannot be ascertained, 30 per cent of the company's adjusted turnover during the breach turnover period (minimum 12 months) for the contravention;

- to give the OAIC enhanced powers to request information and conduct compliance assessments of the notifiable data breach regime under the Privacy Act;
- to give the OAIC new enforcement powers, including allowing the OAIC to require entities to conduct external reviews of their internal procedures and to publish notices about specific privacy breaches to affected individuals; and
- to introduce new information-sharing powers for the OAIC and the Australian Communications and Media Authority, the regulator that oversees telecommunications providers.

Additionally, the Privacy Act's extraterritorial application has been broadened by the passing of the Privacy Bill. The Privacy Act requires entities that are established outside of Australia to meet the obligations of the Privacy Act if they 'carry on business' in Australia; however, the Privacy Bill has removed the former requirement in the Privacy Act for such entities to collect or hold personal information in Australia for the Privacy Act to apply.

More recently, the Attorney General's Report made several proposals to strengthen the enforcement of privacy obligations under the Privacy Act, as well as the notifiable data breach regime under the Privacy Act, including to:

- equip the OAIC with more options to enforce privacy breaches;
- enhance the OAIC's ability to proactively identify and address privacy breaches;
- provide Australian courts with enhanced powers to make orders against entities that have breached their privacy obligations;
- provide new pathways for individuals to seek redress in the courts for privacy breaches, including through a new tort for serious invasions of privacy;
- improve how entities respond when a serious data breach occurs and simplify reporting processes for entities; and
- reduce regulatory complexity by working with states and territories to harmonise key aspects of privacy laws.

The Government's Privacy Response 'agreed' or 'agreed in principle' with the proposals made in the Attorney General's Report regarding enforcement. The Government highlighted strengthening enforcement of privacy obligations as one focus area of its privacy reforms, and stated that its reforms will increase enforcement powers for the OAIC, expand the scope of orders the court may make in civil penalty proceedings and empower the courts to consider applications for relief made directly by individuals.

Law stated - 25 January 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

APP 11 imposes a legal obligation on entities to take steps as are reasonable in the circumstances to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. Apart from this general obligation, there are no mandated IT security standards for the handling of health data in Australia. Some specific standards have been developed, including the Information security management in health using ISO/IEC 27002 and the National eHealth Security and Access Framework v4.0. However, compliance with these standards is voluntary.

The OAIC has published its Guide to health privacy and the Australian Digital Health Agency has published an Information Security Guide for small healthcare businesses. IT service providers who engage with Government health agencies will typically be required to meet certain minimum IT security standards (for example, see the Digital Transformation Agency's Secure Cloud Strategy).

On 22 November 2023, the Australian Government released the 2023-2030 Australian Cyber Security Strategy (2023 Cyber Strategy), which it describes as a roadmap to help realise the Australian Government's vision of becoming a world leader in cybersecurity by 2030. The 2023 Cyber Strategy was accompanied by the 2023-2030 Australian Cyber Security Action Plan (2023 Cyber Action Plan), which supplements the 2023 Cyber Strategy and details the key cybersecurity initiatives that will be delivered over the next two years.

Together, the 2023 Cyber Strategy and 2023 Cyber Action Plan outline significant proposed legislative reforms in respect of ransomware, data retention, critical infrastructure and cyber incident response support as well as other initiatives.

The 2023 Cyber Strategy included the following key proposed legislative reforms:

- the introduction of a no-fault, no-liability ransomware reporting obligation for businesses to give the Government greater visibility of ransomware threats;
- amendments to data retention requirements, with a focus on non-personal data, which aimed to address the risk of an entity holding significant volumes of data for longer than necessary;
- further amendments to the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) (see below), such as to subject telecommunications companies to tougher cyber reporting requirements by moving the security regulation of the telecommunications sector from the Telecommunications Sector Security Reforms in theTelecommunications Act 1997 (Cth) to the SOCI Act;
- limiting Government sharing of cyber information by introducing a limited use obligation for the ASD and the National Cyber Security Coordinator; and
- introducing a mandatory cybersecurity standard for Internet of Things (IoT) devices, a voluntary labelling scheme for consumer-grade smart devices and a voluntary code of practice for app stores and app developers which will communicate

expectations of cybersecurity in software development. The Government has committed A$4.8 million to these initiatives.

Previously, the Australian Government passed the Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI Act) and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act). These Acts implemented the first initiative of Australia's Cyber Security Strategy 2020, which aimed to protect Australia's critical infrastructure providers from cyber threats by amending the SOCI Act. Key reforms made by the SLACI Act and SLACIP Act include to:

- expand the definition of critical infrastructure sectors and assets that are covered by the SOCI Act to include the healthcare and medical sector (among others);
- require mandatory notification of cybersecurity incidents; and
- implement Government assistance and intervention measures that give the Australian Government the power to direct entities to gather information and take certain actions in respect of cybersecurity matters;
- authorise the Australian Signals Directors to intervene in response to cyber-attacks where critical;
- create a new 'positive security obligation' requiring responsible entities to create and maintain a critical infrastructure risk management programme, including consideration of cyber and information security hazards; and
- introduce a new framework of 'enhanced cyber security obligations' that must be complied with by operators of Systems of National Significance (ie, Australia's most important critical infrastructure assets).

Law stated - 25 January 2024

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Organisations should consider the following three key questions.

Consent – do you have adequate consent to collect, use and disclose health data for this purpose? Where health data is collected in addition to personal information, additional consent may be required. The Privacy Act distinguishes between the use and disclosure of personal information for 'primary purposes' versus 'secondary purposes'. The 'primary purpose' is the specific purpose for which the health information was collected. The context in which the health information was collected is relevant to this concept. A 'secondary purpose' is any use or disclosure for reasons other than the primary purpose. Secondary purposes are prohibited, unless the secondary purpose falls within a specific permitted exception.

In the health information context, the most common permitted exceptions are:

- the individual would reasonably expect the organisation to use the information for the secondary purpose, and the secondary purpose is directly related to the primary purpose;
- if the use and disclosure is required to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
- if the use and disclosure is in connection with the provision of a health service or research or if the individual is incapable of giving consent (in each case, subject to specific rules); and
- if required by law or for law enforcement purposes.

Data Systems – do you have appropriate data management systems in place? There are differing legal requirements for the handling of health data and personal information; however, these types of information are most often collected together. It is important to understand which data fits into each category, and to establish distinct data management processes for these different types of data.

Security – do you have adequate security to protect against unauthorised access and misuse? Consider security safeguards that are reasonable in the circumstances.

Law stated - 25 January 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Patentees of digital health-related inventions, which often require computer implementation in one form or another, need to navigate the patentability requirement in Australia. While abstract ideas and computer-implemented inventions are not regarded as patentable subject matter in Australia, patents directed to other aspects of digital health-related inventions such as hardware, telemetry and diagnostic tools may be patent-eligible.

Recently, the Full Federal Court of Australia found that an artificial intelligence (AI) system could not be named as an inventor on a patent application (*Commissioner of Patents v Thaler* [2022] FCAFC 62). The High Court of Australia (Australia's apex court) declined to hear an appeal of this decision (*Thaler v Commissioner of Patents* [2022] HCATrans 199).

Law stated - 25 January 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

The Australian patent system provides the same application process across all technologies, including digital health. There are no specific provisions for digital health technologies. IP Australia (incorporating the Australian Patent Office) is responsible for pre-grant examinations, pre-grant oppositions, re-examinations and amendments to patents and patent applications. As in other jurisdictions, the process of filing to grant can take more than 18 months.

Law stated - 25 January 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Registrable IP rights are available in the form of design rights that safeguard the visual appearance of new and distinctive products, such as wearable devices that incorporate digital health offerings. Design rights are secured through an application process administered by IP Australia and last for five years initially (renewable for another five years).

Additionally, unregistrable forms of IP including copyright, know-how, trade secrets and confidential information may arise in the context of digital health technologies and offerings. Contractual measures (such as non-disclosure agreements) may help to protect the know-how, trade secrets and confidential information, such as secret algorithms in a digital health app, often in conjunction with physical and technological security measures. Copyright arises automatically in some subject matter likely to be integral to digital health offerings, such as in computer code in a digital health app.

Law stated - 25 January 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

Arrangements involving the licensing or assignment of patents are subject to Australian competition laws. In September 2019, the Competition and Consumer Act 2010 (Cth) (CCA) was amended to repeal a section that previously exempted certain IP assignments and licensing arrangements from the full operation of the CCA. Since the repeal of this IP exemption, the Australian Competition and Consumer Commission (ACCC) appears to be taking an increasing interest in restrictions in IP arrangements.

Compliance with the Therapeutic Goods Act 1989 (Cth) (TGA Act) of any relevant IP assets claimed is also likely to be an important practical consideration.

Law stated - 25 January 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

In Australia, there are no bespoke procedures that govern the enforcement of IP rights relating to digital health technologies.

Law stated - 25 January 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

Rules relating to advertising and marketing of digital health products appear in the Therapeutic Goods Act 1989 (Cth), which regulates all therapeutic goods, the Therapeutic Goods Regulations 1990 (Cth), and the Therapeutic Goods (Medical Devices) Regulations 2002 (Cth) (together, the TGA Regulations), which include provisions about advertising therapeutic goods and information about both ingredients and patient information, as well as the Australian Register of Therapeutic Goods.

The Therapeutic Goods (Therapeutic Goods Advertising Code) Instrument 2021 (Cth) (the Advertising Code) ensures that the marketing and advertising of therapeutic goods to consumers is conducted in a manner that promotes the safe and effective use of goods, is socially responsible and does not mislead or deceive consumers. In contrast to the previous iteration of the Advertising Code, the new Advertising Code is far more instructive as to permitted products and prohibited practices. The TGA has also published guidance on social media advertising, the 'TGA social media advertising guide'.

The advertising and marketing of health services, including digital health services, is governed by the Health Practitioner Regulation National Law Act Scheme, with nationally consistent laws passed by each state and territory parliament. To assist providers of health services in Australia understand how national law is to be applied to advertising, the Australian Health Practitioner Regulation Agency has set out guidelines for advertising regulated health services.

In addition, the rules that apply to registered trademarks (contained in the Trade Marks Act1995 (Cth)), and in relation to passing off and misleading and deceptive conduct (torts and the Australian Consumer Law) are relevant in marketing and advertising digital health products and services.

Law stated - 25 January 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

The rules governing e-commerce are the same as the rules governing general commerce and there are no specific rules governing e-commerce for digital health offerings. Similarly, entering into contracts electronically only requires compliance with general contract law and there are no technology-specific rules. As with all customer contracts, businesses must take all reasonable steps to present the contract terms to the customer and ensure that the customer has indicated their consent to those terms. For example, customers accepting terms by selecting a tick box online is equivalent to the customer signing the contract.

Payment rules to note include the Payment Card Industry Data Security Standards (PCI DSS), which are intended to help businesses protect their own and customers' data from breaches and theft. Compliance with the PCI DSS is not mandatory but is strongly recommended given there are legal consequences for data breaches.

Medicare Easyclaim is a Medicare initiative that allows patients to claim and receive Medicare rebates through their healthcare providers. Businesses offering digital health services covered by Medicare may wish to integrate the Medicare Easyclaim system into their practice management software products or alternatively, Medicare Easyclaim can be a stand-alone process via an Electronic Funds Transfer at Point of Sale (EFTPOS) device. EFTPOS providers continue to integrate Medicare Easyclaim into their infrastructure to allow for instantaneous rebates and lodgement of claims.

Some private health insurers provide similar claiming services to Medicare Easyclaim, so that patients do not have to separately claim to their private health insurer to cover a particular cost.

Law stated - 25 January 2024

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Reimbursement is important for creating incentives for the implementation and adoption of digital health products and services in Australia. It is a complex area, and when it comes to digital health products and services under current schemes, it is likely that some products will be covered while others will not.

The Australian Government broadly aims to assist Australians in accessing health services and technologies by subsidising the cost of health-related goods and services, including through the Pharmaceutical Benefits Scheme (subsidies for certain medicines) and the Medicare Benefits Schedule (MBS) (subsidies for certain health services). Telehealth services – being health services provided via videoconference or telephone, instead of via face-to-face consultations – were made temporarily available under the MBS in 2020 in response to the covid-19 pandemic. They have now been made permanently available.

The Australian Government has also increased accessibility to Dexcom G6 Continuous Glucose Monitoring technology. From 1 July 2022, all Australians with type 1 diabetes now have access to Dexcom, which links to a person's smartphone via Bluetooth, providing alerts when blood glucose levels are abnormal. Previously, only individuals with either type 1 or 2 diabetes who met the Medicare Coverage Criteria could access the subsidy.

Private health insurers are required to pay benefits for products listed on the Prosthesis List published by the Australian Government Department of Health (if the product is provided to a patient with the right cover). The current Prostheses List includes various digital health products, such as cardiac implantable electronic devices and cardiac remote monitoring systems. For example, products such as the VISIA AF MRI XT SureScan ICDs, a digital single chamber implantable cardioverter defibrillator, and Cochlear Baha 5 SuperPower Sound Processor, a wireless-enabled smartphone-compatible, fully programmable, digital sound processor for implantable bone conduction hearing systems, are included on the list.

Separately, the Practice Incentives Program eHealth Incentive is a program administered by Services Australia that incentivises general practices to keep up to date with, and to adopt, digital health technology by providing periodic payments to eligible practices.

Law stated - 25 January 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

The digital economy, including consumer data issues in digital health, is an area of priority for the Australian Competition and Consumer Commission (ACCC).

The ACCC continues to commence proceedings focused on misleading and deceptive conduct regarding healthcare products and the use of consumer data in various sectors. For example:

- In December 2023, the Federal Court ordered Fitbit LLC to pay penalties of A$11 million for making false, misleading or deceptive representations to consumers about their consumer guarantee rights in response to claims about faulty devices.
- In September 2023, ACCC commenced proceedings in the Federal Court against dating site eHarmony Inc for alleged misleading statements about the pricing, renewal and duration of online dating memberships.
- In 2023, the Full Federal Court upheld the ACCC's penalty appeal in a case against Employsure Pty Ltd, and Employsure was ordered to pay A$3 million in penalties for making misleading representations in its online ads.
- On 24 October 2022, the ACCC commenced proceedings against Fitbit LLC for misleading consumers around their rights under the consumer guarantee regime in the Australian Consumer Law (ACL). In December 2023, Fitbit admitted that it

contravened sections 18(1) and 29(1)(m) of the ACL, with the Federal Court making final orders on 12 December 2023 in relation to Fitbit's contravention of the ACL. On 5 May 2023, the ACCC accepted a court-enforceable undertaking from vitamin and supplement supplier, Universal Pharmaceuticals Pty, admitting that representations on its Wealthy Health website were likely misleading. Universal Pharmaceuticals Pty undertook to not make such representations unless it has evidence to support the claims, as well as publish a corrective advertisement and offer refunds to customers who purchased the product.

In relation to the ACCC's merger reviews:

- In December 2023, the ACCC commenced an informal review with respect to Westpac Banking Corporation's proposed acquisition of HealthPoint.
- In January 2023, the ACCC announced it would suspend the timeline for announcing a proposed decision date with respect to the proposed acquisition by Cochlear Limited of Oticon Medical A/S, pending receipt of information from the parties. This followed the publication by the ACCC of a Statement of Issues on 1 December 2022 outlining preliminary competition concerns in relation to the proposed acquisition.

More generally, on 27 November 2023, the ACCC released its seventh interim report in its Digital Platforms Services Inquiry 2020-2025, on regulatory reform (DPSI-7). DPSI-7 examined strategies of digital platforms to expand into emerging technologies such as generative AI and digital health services and concerns about the increased risk of harmful practices such as invasive data collection and consumer lock-in practice. The ACCC reiterated its recommendations for a range of regulatory reforms that are likely to impact Australia's digital health industry including new service-specific mandatory codes of conduct for designated digital platforms and new mandatory obligations on all digital platforms to prevent and remove scams, harmful apps and fake reviews, with notice and action requirements and stronger verification of business users and reviews.

On 8 December 2023, the Government said that it recognises the extensive work by the ACCC throughout the Digital Inquiry and agrees that stronger measures are warranted to protect consumers and businesses from harms on digital platforms.

Previous interim reports of the Digital Platforms Services Inquiry 2020–2025 have focused on online private messaging services, mobile app stores, web browsers and general search services, online retail marketplaces, and social media services.

The Australian Government passed the Security Legislation Amendment (Critical Infrastructure) Act 2021 and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022, which implement the first initiative of Australia's Cyber Security Strategy 2020, being to protect Australia's critical infrastructure providers from cyber threats by amending the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act). Significantly, the amendment will impose security obligations on 11 new sectors, including the 'health care and medical' sector.

The recent amendments to the TGA Regulations to exempt certain kinds of clinical decision support software from the ARTG has reduced the regulatory burden for businesses providing this service, and is a significant development affecting the sector.

Since 2019, the Attorney-General had been conducting a review of the Privacy Act (the Review), with several rounds of public consultations. On 16 February 2023, the Attorney General's Report was published, which included 116 proposals for reform. These proposals aimed to make the Privacy Act 'fit for purpose' to 'adequately protect Australians' privacy in the digital age'. On 28 September 2023, the Government released its response to the Attorney General's Report, which offered a fairly modest schedule of agreed reforms, with most matters being deferred to matters of further consultation.

There has been an increased focus on cybersecurity in Australia following two of the largest known cybersecurity breaches in Australia's history: the September 2022 data breach affecting Australia's second-largest telecommunications provider, Optus, which compromised the information of around 9.8 million former and current customers; and the October 2022 data breach affecting Medibank, Australia's largest private health insurance provider. In December 2022, Medibank confirmed that the personal data of up to 10 million customers had been released on the dark web by the criminals responsible for the data breach. As a result of these data breaches and as part of the Review, it is likely that tougher legislative requirements will be imposed in respect of data retention and how much data entities are permitted to collect, and also more stringent requirements on digital health providers given the sensitive data assets they hold.

The National Health (Pharmaceutical Benefits) Regulations 2017 (Cth) have been amended to allow electronic prescriptions under the Pharmaceutical Benefits Scheme. As a result, electronic prescribing has become widely available, with less need for paper prescriptions. Telehealth has also become more prevalent, as from 1 July 2022, the arrangements for the Medicare Benefits Schedule to support patient access to telehealth services were made permanent. These particular developments demonstrate the increased reliance on digital technology in the health sector.

Law stated - 25 January 2024

Susan Jones sejones@gtlaw.com.au
John Lee jlee@gtlaw.com.au
Andrew Hii ahii@gtlaw.com.au

Gilbert + Tobin

Read more from this firm on Lexology

Czech Republic

Barbora Dubanská, **Anna Gelety**, **Marie Kohoutová**
dubanska & co

Summary

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

In recent years, the number of companies active in digital health market in the Czech Republic has been rapidly rising.

The players range from highly innovative private companies which have been established platforms in the healthcare sector, traditional healthcare providers to start-ups.

The services cover telemedicine services, including online booking appointments, telemonitoring of patients or providing prevention programmes.

While modern telemedicine providers focus on easy and user-friendly access to consultation services, monitoring and logistics from the diagnose to the treatment (medical concierge), state-owned specialised hospitals provide programmes focus mainly on specialised telemonitoring of patients with specific diseases.

Start-ups develop various software, including apps for patients, software for healthcare providers or AI diagnostics.

Another important disruptor and driving forces for digital health solutions are IT companies focused on efficient use of electronic health records and both primary and secondary use of data in healthcare. These projects include big data processing and using AI in diagnostics, disease prevention and early detection.

Pharmaceutical companies and traditional medical device manufacturers are also active players and search for ways how to use data available to them. Big data analysis is used in research and development, clinical trials and pharmacovigilance. Patient-support programmes vary from treatment adherence/compliance programmes to digital pills.

Law stated - 30 January 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

Digital health is a trending topic in the Czech Republic and has attracted attention of key stakeholders.

The development of telemedicine and other digital health solutions has been so far decentralised and a bottom-up process. Until recently, the state governed system of healthcare insurance and provision of healthcare has not viewed electronisation of healthcare as a priority and national standardisation of e-health has been rather slow.

Similarly, the legislative framework does not reflect the current state-of-art and healthcare needs.

Another aspect is the low level of cooperation between state and private sector compared to other EU countries.

Some key changes have been initiated by Act No. 325/2021 Coll., on Electronisation of Healthcare (the Act on Electronisation of Healthcare), which was enacted in 2021 and shall be amended in the next months to enable access to electronic healthcare records by patients. However, the draft amendment is rather basic and does not reflect the aims and framework of the draft European Health Data Regulation.

Other efforts evolve around the mandatory standards for healthcare records and reports. Draft standards have been published and are now subject to comments by the medical societies.

Law stated - 30 January 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

There are many promising digital health start-ups that are active in the fields of telemedicine, end-to-end digital medical concierge, workplace health, screening, digital prevention or drug price monitoring. This will likely create an active ecosystem that will be attractive for seed funding and larger investors in the next few years.

In 2021, there was a sale of an 85.9 per cent stake in QUINTA-ANALYTICA. QUINTA-ANALYTICA is a major Czech provider of research and regulatory services for the pharmaceutical, biotechnology and generic industries. The stake was newly taken over by LVA Holding from the portfolio of BBA Capital Partners.

Law stated - 30 January 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

Investor's due diligence of a digital health venture should focus apart from standard due diligence topics on regulatory, data protection, cybersecurity and IP aspects.

Regulatory due diligence is a key part of due diligence of a digital health venture. The extent and focus of the due diligence depend heavily on the nature of the business in question. If the company provides healthcare services, the due diligence should include a review of required authorisations to provide healthcare services. Due record keeping, informed consent processing and maintaining health records should also be checked.

If the product in question is a medical device, compliance with the EU regulation No. 2017/745 on medical devices (MDR) should be reviewed. This review should include

conformity assessment, certification if applicable, clinical trials compliance, technical documentation and packaging and labelling of the product.

Data protection and cyber security due diligence are usually closely connected. Processing health data is regulated by the General Data Protection Regulation 2016/679 (GDPR) and by Act No. 372/2011 Coll., on Healthcare Services (the Act on Healthcare Services). Besides the general issues like proper legal basis for data processing, consent management, provision of information to users or patients and legal relationships with processors, also the compliance of health records should be included within the scope of the due diligence. As the risks related to health data are considerably higher than to general data, the due diligence should focus on the actual internal practice and regimes for data processing with the highest regard to security (both organisational and technical).

Intellectual property is a key asset, especially for a venture basing its business on a product (software, medical device or other). IP due diligence should include trademarks, brands and business names, but especially patents and other forms of protecting the product, as well as proper acquisition of copyrights thereto from contractors and employees. If the product is not protected by a trademark or a patent, possible means of protecting the product should be examined.

Law stated - 30 January 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

Start-ups are most commonly financed by venture capital investment funds, private investors, crowdfunding or bank loans. Small and medium-sized entrepreneurs and companies including start-ups may apply for life sciences or other specialised investment support in the Czech Republic from the government via the CzechInvest agency or from the European Investment Fund.

The government announced in May 2021 that they seek to revive and substantially modernise the economy following the covid-19 pandemic with the help of the National Recovery Plan, which is receiving funding from the EU Recovery and Resilience Facility. Some 2 billion koruna (approximately €79,208,369) should be allocated to digital health.

Law stated - 30 January 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 What principal legislation governs the digital health sector in your jurisdiction?

The Czech Republic is in the process of digitalisation of the healthcare system. Digitalisation is one of the key specific objectives of the Strategic Framework for the development of healthcare until 2030 (Health 2030).

There is, however, no unified legislation governing digital health in the Czech Republic. Digital health services and technologies are governed by laws regulating the respective area of healthcare.

The general framework of eHealth has been laid by the Act on Electronisation of Healthcare, which was enacted in 2021. The Act on Electronisation of Healthcare established an Integrated data interface for communication between healthcare providers. The Integrated data interface includes healthcare registers (including patients, healthcare providers and healthcare workers), identification of healthcare workers, access authorisation and activity records. However, electronic patient health records are not integrated into the data interface and are kept by individual healthcare providers.

The Act on Healthcare Services requires a special e-identity for Healthcare Providers (HCPs), however, the Ministry of Health has not yet introduced this tool. Another hurdle is the lack of interoperability of hospital information systems, which prevents an effective exchange of healthcare records.

Telemedicine services that fall within healthcare services are regulated by the Act on Healthcare Services. In 2022, the Act on Healthcare Services explicitly allowed distance healthcare consultancy services. However, other telemedicine services are not defined and therefore general rules for practising healthcare services apply. The amendment to the Act on Heathcare Services covering telemedicine is now being discussed in the Parliament.

Software as a medical device is regulated by EU Regulation No. 2017/745 on medical devices (MDR) and on a national level by Act No. 89/2021 Coll., on Medical Devices and Act No. 268/2014 Coll., on In-vitro Diagnostic Medical Devices. A medical device (including software) is defined as any device or other article intended to be used for medical purposes such as diagnosis, prevention, monitoring or treatment.

The pharmaceutical industry is also affected by the development of digital health. Act No. 378/2007 Coll., on Pharmaceuticals (the Act on Pharmaceuticals) states an obligation of healthcare professionals to use electronic prescriptions since 2019. The Act on Pharmaceuticals also governs delivery of pharmaceuticals to patients. Only OTC pharmaceuticals can be delivered to patients via a courier and the Act on Pharmaceuticals states many obligations of pharmacies that sell their products online or otherwise allow delivery to patients.

Law stated - 30 January 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

The Ministry of Health is the main supervisory authority for healthcare services. The Ministry of Health sets the course of healthcare policies, initiates legislative development and issues guidelines.

Regional administrative offices issue authorisation to provide healthcare services and have supervisory and enforcement powers over healthcare providers.

State Institute for Drug Control (SUKL) has jurisdiction over pharmaceuticals and medical devices including software as a medical device, delivery of pharmaceuticals and advertisement. SUKL cooperates with the Ministry of Health on digitalisation of the pharmaceutical sector, such as electronic prescription.

Law stated - 30 January 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

There are no specific authorisation regimes for digital health services. General rules apply depending on the individual product or service.

Healthcare services can be provided only by healthcare providers authorised to provide healthcare services. Authorisation is granted by regional administrative offices based on an application. The applicant must among others prove their qualification and technical and personal equipment to provide healthcare services. There are no exceptions for providers of telemedicine services and if such a service qualifies as provision of healthcare it requires an authorisation.

Apps and other software that fall within the definition of a medical device are regulated by MDR. Medical devices are divided into classes (I, IIa, IIb and III) based on their purpose and risks with specific evaluation and registration processes for each class. Prior to putting a medical device on the market the manufacture has to undertake an assessment of conformity (and issue a declaration of conformity). Certain medical devices require a certificate of conformity issued by a notified body. Certain medical devices also require a clinical evaluation.

Law stated - 30 January 2024

Soft law and guidance

9 Is there any notable 'soft' law or guidance governing digital health?

The relevant authorities have not yet issued official guidelines for digital health products and services. The Ministry of Health is currently working with public healthcare providers, professional medical societies, patient representatives and other stakeholders from the public sector to establish a framework for digital health, financing of development of digital health and guidelines for provision of telemedicine services.

Law stated - 30 January 2024

Liability regimes

10 What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

General liability rules apply to digital health products and services.

If a product is faulty and causes damage (material or immaterial), the manufacturer shall pay damages under the Civil Code jointly with importer of the product. The parties can liberate themselves if they prove that the injured party caused the damage themselves or if the product was not manufactured faulty, sold within the framework of business entrepreneurship or the fault could not have been discovered. If a healthcare professional uses a faulty product, they shall pay damages to the injured party and can claim the damages from the manufacturer.

When providing healthcare services, the healthcare provider is liable for any breach of good medicine practices. Civil liability as well as criminal liability in case of harm to health or when resulting in death can apply. Healthcare providers must maintain insurance for professional liability. The issue now under discussion is that there are currently very few guidelines for the provision of telemedicine services in place (one of the exceptions being paediatric telepsychiatry). This brings uncertainty to the healthcare providers who provide telemedicine services.

Law stated - 30 January 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

The Czech legislator relies on the definition of health data provided by the General Data Protection Regulation (GDPR), that is personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status. In practice, borderline cases often occur when data that are not primarily considered health data might be deemed as such based on the context of their processing (eg, if they are kept in the health records under the Act on Healthcare Services). Although the Act on Healthcare Services refers to anonymised data, it does not provide a definition and the GDPR applies. Neither there is a specific definition of anonymised health data in place to simplify medical research.

Law stated - 30 January 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Data concerning health fall within the special categories of personal data, which are granted a higher level of protection under the GDPR. Processing of special categories of personal data is subject to more restrictions and in some cases may lead to necessity to undertake further assessments and usually requires more complex security measures. A detailed regulation on health records is further provided by the Act on Healthcare Services and Decree No. 98/2012 Coll, on health records. Health records can be accessed exclusively by persons and for purposes specified in the regulation. The regulation further governs certain technical and organisational measures that need to be in place to secure the integrity of the records along with fixed data storing periods.

Law stated - 30 January 2024

Anonymised health data

13 Is anonymised health data subject to specific regulations or guidelines?

Properly anonymised data fall outside the scope of the GDPR and are not considered personal data. There is also no any further regulation in place that would apply to anonymised health data. In practice, however, it may be rather challenging to achieve actual anonymisation in full and irreversible way, and the data considered anonymous are often merely pseudonymised. This applies even more to the health data of patients with rare diseases. The population of the Czech Republic is not big enough to enable proper anonymisation in certain cases.

Law stated - 30 January 2024

Enforcement

14 How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The Office for Personal Data Protection (UOOU) has jurisdiction to enforce data protection laws. In its annual report, UOOU provided its final statement on the Ministry of Health's compliance in connection with the EU COVID-19 electronic certificate made available at ocko.uzis.cz as well as relating Te ka and Te ka applications. UOOU focused on the security of personal data processing and found that the Ministry of Health was not compliant as: (1) in connection with the issuance of the original certificates, when the QR code was read by the reader on the mobile device, the data on the certificate holder's insurance number was disclosed; and (2) the Te ka application did not prevent the taking of a screenshot of the display, which is contrary to the purpose of the application (ie, to verify the validity of the certificates), without leaving an electronic trace with personal data on this verification. UOOU further carried out an inspection of the supplier of the online vaccination

booking system, which allowed the display of the insured person's number (and thus birth number) and its subsequent transfer to the USA via the Google Analytics statistical data retrieval tool. The audited person, as an additional processor, was held jointly liable with the controller for breach of article 32(1)(b) of the GDPR because, as an expert, it failed to alert the controller to the inappropriateness of the instruction to set up a system whereby the URL contained the number of the insured person (birth number) and processed it using Google Analytics, thereby leaking URLs including the numbers of insured persons to the extent of approximately 80,000 data subjects. Otherwise, there have not been any notable regulatory or private enforcement actions in relation to digital healthcare technologies.

Penalties imposed under GDPR can amount to €20 million or up to 4 per cent of the total worldwide annual turnover, whichever is higher. Individuals can also file a civil action when their rights to identity or privacy are breached and claim damages.

Law stated - 30 January 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

Act No. 181/2014 Coll., on Cybersecurity (the Act on Cybersecurity) governs cybersecurity issues and protection of critical information infrastructure, important information systems and other systems. Entities listed in the Act on Cybersecurity (including providers of information systems of critical information infrastructure and providers of basic services) must put in place security measures to ensure the safety of the infrastructure, assess their suppliers of IT services and contractually ensure the safety of the services. Entities listed in the Act on Cybersecurity have to report any cybersecurity breaches to the National Cyber and Information Security Agency (NUKIB).

Czech hospitals have been targets of an increased number of cyber attacks. NUKIB reacted to the situation by ordering several entities to follow protective procedures and establish measures to protect Czech healthcare from other attacks. In January 2021, NUKIB redefined the term provider of basic services so that it included more hospitals and providers of healthcare services, therefore imposing higher standards of cybersecurity on these entities. An even wider definition that would include more hospitals is currently being discussed. In 2021, the government announced the Action Plan for Cybersecurity Strategy, which foresees higher protection for providers of healthcare services. In October 2021, historically first sector-wide cybersecurity drill took place. Forty-four hospitals that are providers of basic services took part in the drill, which followed a scenario of a cyber attack. The drill also served as an audit of the cybersecurity measures in place. The Ministry of Health announced its strategy for cybersecurity in August 2021, which foresees sector-specific cybersecurity standards.

In preparation for the introduction of an adequate level of cybersecurity for eHealth services under the Act on Electronization of Healthcare, the Ministry of Health, in cooperation with selected general practitioners, has prepared a Cyber Manual for Doctors.

Law stated - 30 January 2024

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Data protection in digital health is currently a trending topic in the Czech Republic including secondary use of personal data. However, there are currently no guidelines or laws specific to the digital health sector. The use and processing of health data through different digital health solutions are therefore not covered by exceptions set out in article 9 paragraph 2 of the GDPR that refer to national regulation. As a result, consent of the data subject (patient mostly) is necessary. This applies to the secondary use of health data as well. There is no regulation in place that would even enable healthcare providers or research organisations to use pseudonymised data for research unless consent is provided. As to the anonymised data, careful assessment is recommended when conducting the anonymisation. The data should not be prone to singling out, linkage or inference. This is particularly important when making such datasets public. In rare medical cases, the data subject can be relatively simply re-identified based on their diagnosis. This is especially the case when the data is made available to other professionals (specialist articles, conferences) who may have access to additional information enabling them to re-identify the data subject.

Data processing for digital health projects, especially using AI, can bring challenges in the terms of compliance. The use of open AI systems presents a problem to which there is no satisfactory solution yet and therefore should be carefully considered if health data is processed.

Law stated - 30 January 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Software and databases are generally protected by Act No. 121/2000 Coll., Copyright Act (the Copyright Act) as an author's work or by neighbouring rights. In order to be protected, a software, photographs or a database must be the author's own intellectual creation, while other assets must fulfil a higher standard and be a unique outcome of the creative activity of the author and expressed in any objectively perceivable manner including electronic form. Copyrights comprise economic rights (using the work) and moral rights (making changes). Neither of these can be transferred or assigned. As an exception, unless agreed otherwise, the employer exercises the author's economic rights to a work that is a result of the employee's job.

Software as such cannot be patented. In order to obtain a patent covering software, this must be done through so-called computer implemented inventions where the software must have a significant interplay with the physical world due to outer technical effect. The

invention has to be new, industrially usable result of an inventive activity. If the invention is a result of employee's work done within the employee's job, the rights to a patent transfer to the employer by virtue of law unless agreed otherwise in the employment agreement (within three months after the notified date of the originator who created the invention in employment).

IP protection of AI generated products is discussed among lawyers and other experts in the recent years. The law currently does not expressly regulate AI-generated products. However, the opinion of most experts is that an author or inventor can be only a natural person, not AI. This opinion is reflected also by the European Union Intellectual Property Office, which dismissed applications which stated an AI as the inventor.

Law stated - 30 January 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

General patent rules apply also to digital health technologies. The originator of the invention (inventor) or the one to which the originator has transferred rights to the patent can file a patent application with the Industrial Property Office (UPV).

First, UPV conducts a preliminary examination. Eighteen months after the right of priority, the Office shall publish the application and announce its publication in the IPO Bulletin.

Second, UPV conducts a full patentability survey at the request of the applicant. The application, together with the payment of the administrative fee for the complete examination, must be submitted no later than 36 months after the application has been submitted. Based on the full survey, UPV grants a patent.

Law stated - 30 January 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

The Act on Copyright provides protection for an author's work. The copyright in work arises at the moment when the work is expressed in any objectively perceivable form. Authors' rights include moral rights (right to authorship and right to make the work public, as well as the right to make any changes, alterations, translations of the work, and join the work with other elements or include in a collective work) and exclusive economic rights (rights to use, including making copies, distribution, communication to the public and granting a licence to use the work). The author may not waive or transfer his rights. Moral rights shall become extinct on the death of the author; some parts may still be exercised by heirs or collective societies. Economic rights run for the life of the author and 70 years after his or her death.

It is worth mentioning that technical solutions that are not patentable may still be protected by utility models. The key difference is that the Office does not perform a full review as in the case of patents and therefore more subjects qualify for granting the protection. This is balanced by the main disadvantage – anyone can challenge the protectability of the utility model even after its registration, making the protection significantly less secure.

Other IP rights may include designs (protecting the visual appearance of the product, including software) and trademarks used to protect the product's designation, name or logos.

Law stated - 30 January 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

It is important to assess which means of protection apply to the licensed subject matter and proceed accordingly. This means that the license should cover all levels of protection, making sure it remains specific enough (this is especially important in the area of trademarks or patents where the preferred practice is to have them individually listed, rather than covered by a general clause).

Due to Czech specifics, it may be more challenging to license software along with the right to make modifications thereto, since this activity falls under the scope of moral rights that cannot be licensed but rather requires the author's consent. Such consent may not be granted (eg, by the author's employer).

Law stated - 30 January 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

General rules for intellectual property protection apply.

Industrial intellectual property rights are protected by Act No. 221/2006 Coll., on Enforcement of Industrial Property Rights. Owners of rights to industrial intellectual property, their licensee or other entitled person have the following rights as regards persons breaching their rights:

- right to information – request information about the origin of products or services and their distribution;
- remedial measures – claim for desist of placing of products on the market and their retraction, destruction of products and/or materials or means of production,

including preventing providing a service that is used by third parties to infringe the IP rights; and

- damages – claim for payment of damages or unjust enrichment; these can be adjudicated as a flat rate of twice the usual licence fee for unjust enrichment and plus once the usual licence fee for the actual damages.

Similar rights apply to copyright. Enforcement of all IP rights includes the possibility to file for a preliminary injunction.

Law stated - 30 January 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

New regulation of medical devices was enacted in 2021 by and amendment to Act No. 40/1995 Coll., on Regulation of Advertising. Advertising to the general public is permissible only regarding medical devices that do not require a healthcare professional to use them.

The advertisement must:

- clearly state that the product is a medical device;
- include the name of the product;
- include the purpose of the product; and
- include a clear call to read user's manual for the product and safety instructions.

The advertisement must not:

- insinuate that consultation with a healthcare professional is not necessary;
- insinuate that not using the product might lead to harm;
- target persons younger than 15 years;
- use recommendations of healthcare professionals, experts or public figures; and
- exaggerate effects of the product.

Advertisements for products related to health that are not medical devices must not insinuate that the product is a medical device, that the product can improve the health of the user or that not using the product might lead to harm and use recommendations of healthcare professionals, experts or public figures.

Amendment to Act on Regulation of Advertising, relaxes some of the requirements for advertising of medical devices that have proven problematic in practice.

The amendment allows advertising of medical devices to not only 'experts' in the narrow sense of the word (ie, persons authorised to prescribe or dispense), but also to employees of the healthcare provider, whom the amendment equates with experts. This means that medical devices which until now could only be promoted to professionals can now also be promoted to employees of the healthcare provider who do not fall under the legal definition of a professional, such as laboratory technicians.

The Explanatory Memorandum states that this addition has been made:

> in view of the wide variation in medical devices and the people who use them in the context of the provision of healthcare, where the use itself is not only the responsibility of doctors, who were the only ones who fell within the previously stated definition of professional, but also extends to other professional staff, which includes, for example, nurses, biomedical engineers and purchasing department staff.

At the same time, however, the prohibition on gifts is extended to employees of healthcare providers.

Law stated - 30 January 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

General rules for consumer protection concerning e-commerce apply also to digital health services. The consumer has the right to be properly informed about the provider, the service, the price and any related costs as well as their rights as a consumer prior to entering into the agreement. Unfair terms and conditions such as limitations of consumer rights granted by law are prohibited. The provider is obliged to confirm without delay conclusion of the agreement or receipt of an order and provide the consumer with a written agreement and general terms and conditions if applicable. The consumer can withdraw from the agreement without giving reasons within 14 days of concluding the agreement, if the consumer was not informed by the provider, the consumer can withdraw within a year. The consumer cannot withdraw from the agreement on provision of services if the consumer agreed that the services shall be provided before the 14-day deadline expires and the consumer was informed about the fact that they cannot withdraw from the agreement.

Law stated - 30 January 2024

PAYMENT AND REIMBURSEMENT

Coverage

24

Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Currently, there is no systematic framework for reimbursement of digital health products or services in the Czech Republic. There are some exceptions (eg, paediatric telepsychiatry) that is to be reimbursed by the national healthcare system as of 1 January 2024.

Under the current system, health insurance companies reimburse distance consultations with patients (eg, by phone or video call) and the reimbursement varies for individual health insurance companies.

In addition, some health insurance companies reimburse telemedicine services of selected and well-established telemedicine services or pay for digital health products partially (eg, wearables for patients with heart diseases).

Law stated - 30 January 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

Currently, the Act on Electronisation of Healthcare is being reviewed and discussed. While this could be a critical milestone for the development of digital health in the Czech Republic, it has been subject to a lot of criticism.

The aim is the extension of the functionalities of existing central e-health services, in particular extending the functions of the exchange network services as regards the range of subjects using the services as well as in terms of the functionalities of the temporary repository. In addition, it introduces two new concepts: eZkarta and eŽádanka.

eZkarta – this mobile application shall allow patients to view their medical records and access several medical registries. However, there is no obligation for health service providers to keep documentation electronically. Also the healthcare providers will have the option to send documentation to the patient 'within 30 days' and ask the patient to pay for an extract or copy of the medical record.

eŽádanka – shall allow the healthcare providers to file an electronic request for healthcare services for their patients. It is uncertain who is the specific recipient of the eŽádanka, who will pick it up and when, and when it will be deleted from the repository.

As regards the electronisation of healthcare providers, hospitals have different software for processing, storing and archiving health data. Several hospitals were updating their information systems in 2023 and many of them are planning on further modernisation and applying for funding from the National Recovery Plan.

The National Recovery Plan is aiming at the standardisation of medical documentation (such as a discharge report, image report, lab report and patient summary), the creation of

a health portal, a network for the exchange of EHR and operational technical infrastructure for e-health. That is connected to a stronger emphasis on cybersecurity. The ultimate goal is to create a master register of patients, health professionals and healthcare providers.

Law stated - 30 January 2024

Barbora Dubanská bdubanska@dubanska.com
Anna Gelety agelety@dubanska.com
Marie Kohoutová mkohoutova@dubanska.com

dubanska & co

Read more from this firm on Lexology

Germany

Julian Bartholomä, **Daniel Menghin**
Ehlers Ehlers & Partner

Summary

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

The most prominent areas of innovation in the German digital health market are the digitalisation of patient documents, the digitalisation of the interaction between healthcare personel and patients and digital healthcare treatments. In addition the already widely accessible digital health apps, obtainable by prescription and covered by the SHI, services such as telemonitoring of disease and telemedicine will be added to the catalogue of the services covered by the statutory health insurance in the near future. In line with European trends, the national legislator is endeavouring to innovate and facilitate the digital accessabilty of health data for research. The use of AI and Big Data is currently only investigated and not yet implemented in the German Healthcare System.

In recent years, the framework for an effective and efficient use of digital health services has been developed and implemented mainly on a voluntary basis. Among others, the electronic health card, which enables healthcare providers to quickly and easily access patient information, provides emergency information as well as medication regimens, has been implemented. The electronic patient record, which ensures transparency for patients concerning their treatment records and enables more accessible communication between healthcare providers and healthcare institutions has been offered mandatorily to patients by their health-insurance company. Overall, the electronic availability of the data has shown to lead to significant time saving regarding the procurement of information and can thus sustainably improve personal medical treatment in the future. Recently the German legislator has been working on some amendments to existing laws to provide for a mandatory use of digital health services such as the electronic patient record or the electronic prescription.

With regards to the digital healthcare of patients, digital health applications (DiGAs) are already well established and digital care applications (DiPAs) may now be added to the benefits catalogue of the SHI. DiGAs are low-risk medical devices (risk class I and IIa) that perform a support function in the detection, monitoring, treatment or alleviation of disease or injury and disability. Recently, the legislator has decided to allow the use of higher-risk medical devices (risk class IIb). DiPAs, on the other hand, are not medical devices but other applications based on digital technologies. Such applications are used in the care of people in need of care or the interaction of people in need of care with their carers or relatives. The applications aim to reduce the impairment of both the independence and the abilities of the person in need of care.

Ultimately, telemedicine, which has made considerable progress in recent years, shall become an integral part of patient healthcare. In German legal doctrine, telemedicine is understood as medical consultation or treatment with the aid of telecommunications media. The aspect of medical consultation in particular is intended to be used even more extensively in the future.

Key players enabling, forging and supervising these innovations are government institutions such as the Federal Ministry of Health, the Federal Ministry of Labour and

Social Affairs and the Federal Institute for Drugs and Medical Devices. Further, there are regulatory authorities in the form of public bodies, such as the National Association of Statutory Health Insurance Physicians (GKV-SV) or of special forms such as the Federal Joint Committee (G-BA), which play a key role within the SHI, especially concerning the supply of digital health products. Finally, gematik GmbH, a limited company under the control of the German government, the GKV-SV and other organisations such as the Federal Association of Statutory Health Insurance Physicians, the German Hospital Association and the Federal Association of Physicians play a significant role within the digitalisation of the German healthcare system.

Key areas for private healthcare businesses and developers of digital health systems include telehealth and virtual health services. These now include numerous services in areas such as nutritional counselling, rehabilitation support and psychological support. In particular, the aspect of personalised treatment, especially with the help of digital health systems, is becoming increasingly important.

Law stated - 1 February 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

The investment climate for digital health technologies is guided by several provisions in the German legal system that are aiming to stay as simple and investor-friendly as possible while simultaneously fulfilling all the necessary steps of approval. For example, there is a fast-track procedure provided by section 139e of SGB V for the manufacturers of digital healthcare technologies to get approved and listed by the Federal Institute for Drugs and Medical Devices within three months of submitting their completed application. Through this application process, digital health technologies can become part of those medical services refunded by the SHI.

Nevertheless, the market for medical products in Germany is highly regulated and challenges can be found in legislation that have not been modernised yet. In addition, start-ups that are widespread in Germany and cover almost every aspect of digital health services face challenges concerning long processes and slow offer scaling due to the highly regulated market. Since they have short financing cycles and considerable financial pressure from investors, they can only focus on areas of the healthcare market that are accessible in a relatively fast manner such as DiGAs.

Law stated - 1 February 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

In Germany, the acquisition activities of strategic investors are still small in volume and number but, in recent years, have increased rapidly and are continuous. During 2015–2017, the first significant acquisitions in Germany could be registered. Recently, the German government, together with the federal states, facilitated a hospital future fund, which it endowed with €4.3 billion to promote future investments. Moreover, start-ups are an important part of Germany's healthcare digitalisation and are funded by state projects as well as private investors.

The number of company acquisitions in the European digital health sector fell significantly last year. This also applies to Germany. The most active buyer of European digital health companies is the German CompuGroup Medical (CGM). Since 2013, the Koblenz-based company, which itself offers software for clinics, medical practices and pharmacies, has acquired 25 companies. The most recent acquisition is the Cologne-based company mDoc, which specialises in the development of patient portals.

Law stated - 1 February 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

Against the background of digital health products, especially DiGAS being medical devices, reference can be made to due diligence specifics of this type of product. In particular, aspects of CE certification, the manufacturing process and the design of the vigilance system, the national pricing of medical devices and the advertising of medical devices, should be emphasised.

A special feature within the framework of the DiGA is the legally required topicality with regard to data protection and data security of the health application and the quality, safety, functional capability and interoperability of the medical device. It should be noted that such requirements must not only be fulfilled within the framework of the inclusion of a DiGA in the directory pursuant to section 139e of SGB V but as long as the DiGA is supplied within the SHI. In this regard, it is important to check which measures have been taken to implement these requirements and keep them up to date.

Finally, a company's compliance with data protection regulations must also be considered. In this context, it is important to check which personal data, in particular special categories of data, are collected, processed and stored. Special consideration must be given to cooperation with companies that are not based in EU member states or contracting states of the European Economic Area.

Law stated - 1 February 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

In Germany, digital health ventures are often not only financed by large international investors, but by the pharmaceutical industry and health insurance companies as well.

In addition, the German government is also involved in financing digital health sector innovations in the form of an investment fund. Section 92a of SGB V forms the legal basis in this regard. Although the innovation fund is not only applied to eHealth, the majority of the forms of care funded with it originate from the area of telemedicine and eHealth.

Participation in the innovation fund requires an application. The decision is made by the Innovation Committee at the G-BA. Members of the committee are, on one hand, representatives of the self-administration (the GKV-SV) and, on the other hand, representatives of the Federal Ministries of Health and Education and Research. The amount of funding associated with the Innovation Fund, which was awarded during 2016–2019, was €300 million. Some €200 million has been provided for 2020–2024.

Law stated - 1 February 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 | What principal legislation governs the digital health sector in your jurisdiction?

The German legislator has enacted multiple laws and legal provisions to govern the digital health sector within the Statutory Health Insurance (SHI), referencing in particular digital health applications (DiGAs) and the telematics infrastructure (TI)).

The legal basis is found in Social Code (SGB) V. The E-Health Act of 2015 already paved the way for a comprehensive digitisation of the German healthcare system. Subsequent laws, such as the Patient Data Protection Act 2020 (PDSG) and the Digital Supply and Care Modernisation Act 2021 (DVPMG) have significantly changed and developed this legal basis to enable and secure digital health developments. Most recently, the legislator has been working on the Act to Accelerate the Digitalisation of the Healthcare System and the "Act on the Improved Use of Health Data. These are aimed at a broader implementation of digital health services in the daily healthcare of patients and at facilitating the use of health data respectively.

Additional key legislation with a certain relevance within the digital health sector are:

- Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR);
- the Federal Data Protection Act;
- the Act Against Unfair Competition; and
- the Act on the Advertising of Medicinal Products.

The above-mentioned pieces of legislation, although not specifically enacted to face the challenges that arise from the digital health sector, regulate a variety of consumer protection issues.

The most relevant provisions for digital health in the context of the SHI (amended by the E-Health Act, the Appointment Service and Supply Act, the Drug Supply Safety Act, the Digital Care Act, the PDSG 2020 and the DVPMG to improve and expand the digital health sector) include:

- sections 306 and 334 of SGB V on TI and its applications;
- sections 33a, 134 and 139e of SGB V on DiGAs;
- section 20k of SGB V on the promotion of the digital health literacy of insured persons within the SHI;
- sections 40a and 78a of SGB XI on digital care applications (DiPAs); and
- section 68c SGB V on the promotion of digital innovations by the Associations of Statutory Health Insurance Physicians and the Federal Associations of Statutory Health Insurance Physicians.

In addition, Regulation (EU) 2017/745 (the Medical Devices Regulation) (MDR) requirements apply to medical devices and their manufacturers or distributors. The Artificial Intelligence Act was announced in April 2021 and has yet to be adopted by the European Parliament and EU member states. It foresees new regulations on artificial intelligence based on four risk classes. The exact timing of implementation and any adjustments cannot be foreseen at this time.

Law stated - 1 February 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

Digital healthcare in the German healthcare system is characterised by the interaction of three components that represent a part of the German digital healthcare system:

- the TI;
- DiGAs and DiPAs; and
- telemedicine on the part of physicians.

First, it is the responsibility of the Federal Association of Physicians and the Associations of Physicians of the Individual Federal States to permit the use of telemedicine by physicians under professional law. The Federal Medical Association, in its role as the key organisation for medical self-administration, is responsible for monitoring the compliance of medical standards to prevent medical malpractice. The recent reform efforts shown by the German legislator indicate that an increase in the use of telemedicine is intended and that it is supposed to become an integral part of the German healthcare system.

With regard to the digital structure in the SHI system, the gematik GmbH, as a company in which the German state, the National Association of Statutory Health Insurance Funds (GKV-SV) and the main organisations for SHI-accredited physicians, hospitals and

pharmacists hold a stake by law, is responsible for the establishment and expansion of the digital structure in the German healthcare system (namely, the TI), for its secure operation and the approval of components (see sections 306 and 311 of SGB V). New applications, components and services in the TI must be evaluated and approved by gematik GmbH. The role of gematik GmbH is to be classified as highly relevant because a large part of the German population is in the SHI system.

According to the MDR, a CE certification must be obtained for medical devices, generally with the involvement of a notified body.

Regarding DiGAs and DiPAs, a licensing and authorisation procedure is carried out by the Federal Institute for Drugs and Medical Devices (BfArM), an independent federal division of the Federal Ministry of Health. In addition, the BfArM also supervises DiGAs and is responsible for patient concerns and complaints to eliminate errors and secure health standards. Within the SHI, the Federal Joint Committee is authorised to establish mandatory guidelines, which concern digital health services as far as they are listed as billable services in the state insurance system.

As far as reimbursement procedures are concerned, both the GKV-SV and the representatives of the manufacturers of DiGAs and DiPAs play an important role (see section 134 of SGB V and section 78a of SGB XI).

Law stated - 1 February 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

The provision of a service within the framework of the TI in the form of a component or a service of the digital supply structure requires authorisation from gematik GmbH. The basic criterion for the granting of authorisation for the provision of services for the benefit of the TI in the form of components and services is the fulfilment of security requirements in the form of availability, integrity, authenticity and confidentiality.

The applications of the TI (including, eg, the electronic patient record or the electronic prescription) as such are also subject to authorisation according to section 311 of SGB V as services of the application infrastructure (see section 306(2)(3) of SGB V) and consequently as part of the telematics infrastructure. They must demonstrate security requirements in the form of interoperability, availability, integrity and confidentiality. Special consideration in this context is given to access rights to personal data stored in the TI by means of applications. The primary criterion here is always the existence of the consent of the data subject and the strict limitation of the purpose of the processing.

A DiGA is (still) defined as a low-risk medical device under section 33a of SGB V. Both class I and class IIa medical devices are legally defined as low-risk classes. For a DiGA to be used in Germany, it must meet MDR requirements. Further requirements, such as inclusion in a directory according to section 139e of SGB V, apply to the provision of services at the expense of the SHI.

A DiPA, on the other hand, represents a separate group of technological applications. According to the definition in section 40a of SGB XI, a DiPA does not belong to the group of medical devices. Consequently, DiPAs are not subject to MDR requirements. However, DiPAs are also subject to the requirement of inclusion in a directory maintained by the BfArM so that they can be reimbursed by the SHI.

Finally, for the sake of completeness, reference must be made to the provision of digital services by physicians in Germany in the form of telemedicine. The limits of telemedicine are set primarily in the professional law of the physician as well as in the billing of the corresponding activities within the framework of the SHI. Professional law requires that the provision of medical services be carried out with diligence. It was not until 2018 that the comprehensive applicability of telemedicine in medical professional law was permitted due to an amendment in section 7 of the Model Professional Code for Physicians (MBO-Ä) that opened up the possibility of 'exclusive consultation or treatment via communication media'. Temporal and local synchrony is thus no longer mandatory. However, the definite design of the medical service requires individual consideration, since section 7 of the MBO-Ä also requires that the medical service is carried out carefully, in particular with regard to the assessment of findings, consultation, treatment and documentation. On one hand, the physician must be aware of the special features of telemedicine, and on the other hand, the patient must be informed of them during the consultation. Since 2016, ever more telemedicine services have been included in the Schedule of Fees of Statutory Medical Insurance Physicians for Outpatient Care.

Law stated - 1 February 2024

Soft law and guidance

9 | Is there any notable 'soft' law or guidance governing digital health?

Concerning digital health, there is a 'soft' law to be found in the MBO-Ä guided by the German Medical Association. Essentially, it is a guideline published by the committee of all physicians in Germany that should regulate and secure a uniform medical standard and patient provision. Section 7 IV of the MBO-Ä regulates how, and under which circumstances, physicians can provide their remote healthcare services. Mainly, they are advised to inform their patients fully about the remote situation and use this communication form only if it is suitable for a specific medical treatment or consultation.

Further, there is guidance published by the BfArM concerning the fast-track procedure by section 139e of SGB V, which must be followed by inventors, service providers and practitioners.

Law stated - 1 February 2024

Liability regimes

10 | What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

The Product Liability Law applies to medical products, including digital health products, making both products fall under the no-fault liability regime, which is the strictest liability regime established in German law and enables consumers to claim damages against the manufacturer in the case of body, health and property damages. Further, the implementing act of medical products, the Medical Device Law Implementation Act, defines the responsibilities and prohibitions of marketing, distribution and production of medical products that are relevant to determine due diligence and burden-of-proof regulations. In addition to these laws, the civil liability regime applies as well, which includes special regulations concerning treatment contracts between physicians and patients and the claim in tort. Article 11 of the MDR provides that medical devices, including digital health products, can only be put on the market if the manufacturer is either established in an EU member state or provides an EC representative to ensure that liability claims can be implemented. Claims for damages can also be derived from the GDPR.

Law stated - 1 February 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

Health data is defined in section 46(3) of the Federal Data Protection Act (BDSG). It states that information related to the mental and physical health of a natural person as well as on the healthcare services used are health data if the information on a state of health can be derived from them. However, this definition corresponds word-for-word with the definition of health data found in article 4(15) of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR). The same applies to genetic and biometric data.

A definition of anonymisation is not found in the BDSG. In German legal doctrine, with reference to the EU legal basis, it is pointed out that in relation to pseudonymisation, this is an increased form of making the individual unrecognisable. Such a form of anonymisation is only possible in principle, depending on the type of health data. For example, anonymisation of genetic data is, by definition, not possible.

Law stated - 1 February 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

In principle, the level of protection of health data corresponds to the standard set by the European Union. Against this background, the data protection of health data differs in particular from the level of protection of data that is not counted among the special categories of personal data. However, in deviation from, or in addition to, this EU standard, on one hand, an amendment of the permissive elements of article 9(2) of the GDPR by

section 22 of the BDSG can be emphasised. According to this, health-related data can also be processed in Germany by non-public or public bodies, among other things, if social security rights require this, for the purpose of preventive healthcare and healthcare by medical staff or staff with corresponding confidentiality obligations, or if the public interest requires this. For example, multiple federal laws, such as the Infection Protection Act, the Medical Devices Act or the Social Code (SGB) V, provide for exceptions in favour of the processing of personal data. Appropriate measures for the protection of personal data must be implemented within this framework.

Such a requirement for appropriate measures can be seen both in the special legal regulations on data protection in SGB V, especially in the implementation of the healthcare system's telematics infrastructure (TI), digital health application (DiGA) and digital care application systems in Germany.

SGB V devotes a separate 10th chapter to data protection within the framework of the Statutory Health Insurance (SHI). The data that may be processed by health insurance funds and the SHI-associated physicians is regulated according to its purpose.

With regard to the components and applications in the TI, it is regulated in section 306 et seq of SGB V that the entire structure can only be operated with those components that can guarantee the requirements for the protection of personal data. Since the data processed in the TI are likely to be special categories of data, the demands on data security are correspondingly high (for this, see the explicit regulation in section 306(3) of SGB V). In particular, a comprehensive level of protection is ensured through complete subsidiarity for data responsibility for processing in the TI. Section 306(5) of SGB V stipulates that gematik GmbH is responsible for the processing of personal data insofar as it determines the means of processing and no other person responsible for a specific situation results from the legal regulations.

In accordance with these standards, the requirements for data protection regarding health data when using digital health offerings in the SHI are highly regulated. At present, inclusion in the directory according to section 139e of SGB V is only possible if the DiGAs can guarantee data security.

In future, the requirements for the secondary use of certain health data, particularly in research, will be eased (Act on the Improved Use of Health Data). In some cases, for example, it should be possible to make secondary use of health data without prior consent by the data subject. Protective measures, such as pseudonomyisation and anonymsiation must be taken whenever possible.

Law stated - 1 February 2024

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

Anonymised health data is not subject to any special legal regulations. As already evident from the EU requirements, the application of data protection law is not appropriate, even for special categories of personal data, if no identification of the person is possible based on the available data, even if third-party information is used. However, the Federal Ministry for

Economic Affairs and Energy, in particular, argues that it is difficult to completely anonymise health data.

For this reason, guidance on the anonymisation of health data was published in 2018. Although the Federal Ministry also points out that it can only be decided in individual cases when anonymisation was successful, it nevertheless provides guidelines for action. For example, randomisation, generalisation, removal of rare attributes (rare diseases) and especially the combination of these techniques, are recommended.

Law stated - 1 February 2024

Enforcement

14 How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

Pursuant to section 9 of the BDSG, the Federal Commissioner for Data Protection and Freedom of Information (BfDI)) and the committee of Independent German Federal and State Data Protection Supervisory Authorities are responsible for enforcing the provisions on data protection. While the BfDI is responsible for supervising both public bodies and private companies, the data protection authorities of the federal states are responsible for supervising individual and legal entities in the non-public sector. In accordance with the provisions of the GDPR, in particular articles 57 and 58, both the BfDI and the data protection authorities of the federal states have the corresponding powers to monitor and enforce data protection provisions. This also applies to health data in particular.

The BDSG further provides for criminal law provisions for the commercial violation of data protection provisions. The acceptance of remuneration or the intention to enrich oneself or a third party by violating data protection provisions constitutes criminal offences.

Regarding the violation of health data in the context of the use of health technologies, no relevant decisions by the data protection authorities of the federal states or the BfDI are known to date.

Law stated - 1 February 2024

Cybersecurity

15 What cybersecurity laws and best practices are relevant for digital health offerings?

Cybersecurity in the context of the use of DiGAs is already regulated in the SGB V as well as in the DiGA-V. Both the SGB V and the legal ordinances on DiGAs (DiGA-V) oblige the implementation of sufficient measures to maintain data security according to the state of the art. Additionally, from 1 January 2025, the manufacturers of DiGAs must fulfil the requirements of the Federal Office for Information Security according to section 139e(10) of SGB V and acquire the corresponding certificate. The Federal Office for

Information Security already provides specifications for the implementation of the data security requirements within the framework of the technical guideline BSI TR-03161.

In addition, the application of special regulations may also be required due to the classification of the healthcare sector as a component of a critical infrastructure area. Although the healthcare sector is generally considered an area of critical infrastructure within the scope of section 6 of the BSI Criticality Ordinance, the use of DiGAs is not directly covered by it. However, their use in the context of inpatient treatment, for example, is very much subject to the BSI Criticality Regulation. In such a case, section 8a of the BSI Act applies, which obliges the operator of critical infrastructures to maintain appropriate organisational and technical precautions to ensure the availability, integrity, authenticity and confidentiality of the systems, components and processes. Digital health applications and TI services and applications may be particularly relevant as a component of such structures.

A directive in accordance with section 75b SGB V was issued to ensure cybersecurity in the area of telemedical service provision by physicians as part of SHI services.

The Artificial Intelligence Act was announced in April 2021 and has yet to be adopted by the European Parliament and EU member states. It foresees new regulations and safety requirements on artificial intelligence based on four risk classes.

Law stated - 1 February 2024

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

When processing health data, it is first necessary to record the responsibility for processing in a structured manner according to the definition of the GDPR. In particular, joint processing requires that responsibilities are explicitly separated within a contractual agreement. There is no ownership of health data in German law, which is why individual responsibilities must be clearly regulated between the parties.

Even before the processing of personal data, especially special categories of data, the establishment of technically secure and resilient systems is to be considered obligatory. This corresponds to the legal requirements for approvals both within the framework of the TI and for approvals of digital health and care applications.

Finally, regarding a subsequent secondary use of health-related data, possibly for research purposes, it is currently still advisable to obtain broad consent from the data subject at the beginning of the data processing. The possibility for such processing based on the informed consent of the data subject was created in the Data Protection Conference (the committee of Independent German Federal and State Data Protection Supervisory Authorities) on 15 April 2020. Within the framework of the conference, a standardised template for patient consent was approved within the resolution framework. In the near future, the data subject's consent might not always be necessary.

Law stated - 1 February 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Section 1 of the German Patent Act states that patentability requires that an invention must pertain to a field of technology and be new, inventive and industrially applicable. Further, it must be a human-made invention as an artificial intelligence-generated invention does not qualify for a patent. Accordingly, for digital health inventions, section 1(3)(3) of the German Patent Act is important as it states that computer programs, as such, are not patentable. This includes software, algorithms and databases because, according to the Federal Court of Justice, they lack technological innovation. To be patentable, they must exceed the basic form of computer program and data processing.

Therefore, the technical character of an invention gains particular importance. For example, computer-implemented inventions are patentable if a programmable device such as a computer, smartphone or smartwatch is used and features the invention.

Law stated - 1 February 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

Since Germany is a member state of the European Union there are two possibilities for patent registration. The invention can be filed with an application by the German Patent Office or by the European Patent Office to achieve an EU patent. In general, the registration for digital health technologies is the same as for any other invention stemming from other fields. After submitting the complete applications, they are published within 18 months, provided that the registration fees are paid and the patent conditions are met. Upon grant, third parties may file an opposition or a nullity action after passing the opposition period. The granted patent will last for 20 years. In the evaluation process, the German Patent Office applies a three-step approach to assess technical character, working mechanism and surplus value as well as the consideration as new and inventive over the state of the art.

Law stated - 1 February 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Several other IP rights might be relevant when manufacturing and placing a digital health product on the market. In addition to the patent, a trademark application can be filed to identify the product of an entrepreneur, which grants exclusivity rights on the basis of which the product can be protected from the products of other entrepreneurs. Trademark protection can be enforced by means of injunctions and claims for damages. Further, there is a claim for removal and destruction, as well as for information about the origin of the illegally marked products.

The protection of computer programs (software) is also explicitly provided for in section 69a of the Copyright Law. This extends to the forms of expression of a computer program, provided that these are an independent intellectual achievement of the author, but not to the ideas and principles underlying them. Copyright is protected within the framework of prohibitions on reproduction and claims for remuneration in the event of an infringement of the prohibition on reproduction. In addition, the author is entitled to injunctions, destruction and removal of the unlawfully produced work.

Moreover, the Design Act offers the possibility of protecting two- or three-dimensional products or their parts if they are new and innovative. This protects the design of a product. In the case of digital health applications (DiGAs), for example, the external structure or the interface. These rights are also enforced through claims for injunctive relief, removal and destruction of the unlawfully created product.

Law stated - 1 February 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

When licensing IP rights in the field of DiGAs, particular attention must be paid to the sufficient contractual regulation of the respective obligations between licensee and licensor. In addition to necessary regulations regarding the continuous compliance with possible standards with regard to data security and the implementation of data protection provisions, this also concerns the possible handling of trade and business secrets. An obligation to maintain confidentiality should be provided for with regard to such information. In addition, the territorial limits of licensing rights, especially in the manufacture and distribution of medical devices, should be taken into account.

Law stated - 1 February 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

The procedures for enforcing IP rights relating to digital health products are no different from the enforcement of IP rights in other sectors. Patent rights as well as design rights, trademark rights and copyrights give rise to a claim for injunction, removal, destruction, damages or recovery of the unlawfully obtained (eg, from the payment of a licence fee). These claims can be asserted before civil courts and before regional courts in particular. In all cases, a possible statute of limitations of the claims must be taken into account if a period of three years from the date of knowledge of the infringement has elapsed.

Law stated - 1 February 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

There is no special provision that regulates the advertising of digital health products. However, given that digital health products may be considered medical devices, the Act on the Advertising of Medicinal Products (HWG) still applies to in vitro diagnostics and partially to medical devices, but Regulation (EU) 2017/745 (the Medical Devices Regulation) (MDR) or article 7 of the MDR is most relevant. With the introduction of the MDR, permissible claims for medical devices are now regulated at the EU level for the first time. Article 7 of the MDR covers labelling, instructions for use, making available, putting into service and the advertising of devices that may be misleading through the use of text, names, trademarks, pictures and figurative or other signs. The Act Against Unfair Competition (UWG) also applies. Further, several regulations governing professions, such as the Medical Association's professional code or industry guidelines, such as the Association for the Voluntary Self-Regulation of the Pharmaceutical Industry Code of Conduct, may govern the advertisement of medical devices as well. As a general principle, an activity generally only falls within the scope of the HWG or article 7 of the MDR if it is product-related and intended to increase sales of a product. Company-related activities are governed by the UWG.

Generally, product-related advertisements (see section 3 of the HWG and article 7 of the MDR) and company-related advertisements (see section 5 of the UWG) addressed to healthcare professionals must not be misleading or unfair, which means the promotional statement must be correct and, if necessary, veri able.

Misleading also means failing to inform the user or the patient of a likely risk associated with the use of the device. The MDR, HWG and UWG contain definite examples of misleading or unfair advertisements.

Although section 9 of the HWG states that no advertisement regarding telemedicine in general, and the use of digital health products enabling telemedicine in particular, may be admissible, this does not apply to products, whose application corresponds to the standard of medical practice.

Law stated - 1 February 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

There are no individual requirements for digital health products provided for in the provisions regulating e-commerce. In e-commerce, general legal principles, such as the German Civil Code, the German Commercial Code and the Law Governing General Terms and Conditions apply without restriction. Sections 312c et seq of the German Civil Code apply in particular to online trade. These state that in distance contracts where the consumer has no opportunity to see the product, special information obligations and special rights of withdrawal apply. For example, information must be provided about the essential characteristics of the goods, the total price of the goods must be presented sufficiently clearly, payment and delivery conditions must be clearly explained and digital content and protective measures must be sufficiently explained.

Law stated - 1 February 2024

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

The use of digital health applications (DiGAs) and digital care applications (DiPAs) within the framework of, and at the expense of, the Statutory Health Insurance (SHI), requires a separate approval procedure. Digital health applications may only be provided at the expense of the SHI pursuant to section 33a of Social Code (SGB) V if they have been included in the directory pursuant to section 139e of SGB V. The inclusion of DiGAs in this directory, which is maintained by the Federal Institute for Drugs and Medical Devices (BfArM), an independent federal division of the Federal Ministry of Health, takes place upon application and requires proof that the digital health application meets the requirements for safety, functional capability, quality, interoperability and the requirements for data security and data protection according to the state of the art. In addition, proof of a positive care effect, which is either expressed in a medical benefit to the patient or the patient-relevant improvement of the structure and procedures of care, is required. If immediate proof of a positive healthcare effect is not possible for the manufacturer of the medical device, inclusion in the directory according to section 139e of SGB V can take place on a trial basis for a maximum of one year if it is plausibly proven with the help of a scientific evaluation concept that such an effect exists. Regardless of the type of inclusion, the DiGA can be prescribed and used at the expense of the SHI. The DiGAs already included in the catalogue can be found in the DiGA directory.

Negotiations on the reimbursement amount of DiGAs are conducted by the parties (the manufacturer and the Federal Association of Statutory Health Insurance Physicians (GKV-SV)) based on a framework agreement concluded between the GKV-SV and the relevant organisations of manufacturers of DiGAs formed to represent the economic

interests. Criteria for the assessment of the reimbursement amount are the extent of the positive care effect, the reimbursement amount in reference countries as well as the success of the DiGA in care. In December 2021, the parties to the Framework Agreement found agreement on a methodology for determining thresholds below which there is no need to negotiate a reimbursement amount, and for determining maximum prices that represent the maximum reimbursement amount for a DiGA.

According to section 40a of SGB XI, DiPAs are eligible for reimbursement if the BfArM has included the DiPA in the directory, according to section 78a of SGB XI. Inclusion in the directory takes place after a corresponding application by the manufacturer. The BfArM then assesses whether the requirements for safety, functional capability, quality and data protection or security are met. The quality of a DiPA is legally defined. These include accessibility, age-appropriate usability, robustness and consumer protection. In addition, the DiPA must have a nursing benefit. Before the DiPA is used, the long-term care insurance fund decides upon application whether the DiPA is necessary in a specific case of long-term care.

In addition to medical professional law, the reimbursability of telemedical services restricts the offer of such services. In particular, reimbursement of telemedical services within the SHI framework is only possible if they are included in the Schedule of Fees of Statutory Medical Insurance Physicians for Outpatient Care according to section 87 of SGB V. For example, the provision of telemedical services in the area of monitoring patients with a defibrillator or cathode-ray tube system, the assessment of findings from X-rays or computerised tomography scans, the obtaining of teleconsultations or video consultation hours are considered reimbursable services in the SHI. Further detailed requirements for the provision of telemedical services within the framework of the SHI can be found in the framework agreement of the GKV-SV and the National Association of Statutory Health Insurance Physicians.

The amount of telemedical services or teleconsultations that a pyhsician may provide at the expense of the statutory health insurance may not exceed the limit of 30 per cent of the total number of services. In addition, the number of treatment cases in which services are provided exclusively within the framework of a video consultation must be limited to 30 per cent of all treatment cases of the service provider participating in SHI-accredited medical care.

Regarding the reimbursability of digital services for privately insured persons, reference must be made to the individual design of such insurance contracts according to section 193 of the Insurance Contract Act.

Law stated - 1 February 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

The German legislator has essentially completed their work on the Act to Accelerate the Digitalisation of the Healthcare System and the Act on the Improved Use of Health Data at the end of last year. It is expected that these laws will be promulgated and come into force in the first few months of 2024. It is expected that the regulations contained therein, for example on the secondary use of health data or the expansion of the possible applications of higher-risk digital health applications, will significantly shape the German digital health market in the near future.

Law stated - 1 February 2024

Ehlers Ehlers & Partner

Julian Bartholomä j.bartholomae@eep-law.de
Daniel Menghin d.menghin@eep-law.de

Ehlers Ehlers & Partner

Indonesia

Winnie Yamashita Rolindrawan, **Mutiara Kasih Ramadhani**, **Gabriela Eliana**
SSEK Law Firm

Summary

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

The digital health market in Indonesia falls under the regulatory framework for telemedicine. Indonesia Law No. 17 of 2023 regarding Health (Health Law) defines telemedicine as the provision and facilitation of clinical services through telecommunications and digital communication technologies.

The concept of telemedicine was not governed by the previous health law that was revoked by the current Health Law. Nonetheless, the term 'telemedicine' was previously stipulated in Minister of Health Regulation No. 20 of 2019 regarding the Organization of Telemedicine Services through Health Service Facilities (MOH Reg. 20/2019). MOH Reg. 20/2019 defines telemedicine as the provision of long-distance health services by professionals utilising information and communication technology, although the regulation does not directly regulate healthcare services to patients. Instead, it focuses on digital interactions among healthcare facilities, such as hospitals. Subsequent regulations have since then allowed doctors to practice medicine through electronic systems.

One of the most prominent areas of innovation within the digital health market in Indonesia is the emergence of mobile health applications providing telemedicine and remote consultations with healthcare providers and practitioners. Private investments in the Indonesian digital health market often target telemedicine electronic applications, typically operated by companies engaged in commercial web portal businesses (digital platforms).

The recently issued Health Law stipulates that healthcare facilities and medical/healthcare professionals may engage in the provision of telemedicine or otherwise cooperate with digital platforms to provide clinical services to patients, *provided that* the clinical services are carried out by the medical or healthcare professionals.

Several key players active in the Indonesian digital health market include:

- Healthcare Providers: Halodoc, Alodokter, KlikDokter, SehatQ, Good Doctor, Riliv and GrabHealth are several notable digital platforms providing digital health services, including telemedicine services, in Indonesia. These digital platforms must engage healthcare providers such as medical personnel. Healthcare facilities have also engaged in facilitating healthcare services to patients by digital means.
- Pharmaceutical Industry: Pharmaceutical companies are engaged in the sale of pharmaceutical products via digital platforms, contributing to the accessibility of medications through online channels. Digital platforms typically also engage the pharmaceutical industry, pharmaceutical wholesalers and pharmacies to allow platform users to buy pharmaceutical products (prescribed or over the counter).
- Government:

1.

Ministry of Health (MOH): regulates and oversees health-related policies, including those related to digital health, telemedicine services and health information systems.

- Food and Drug Authority: regulates the distribution of medicines and pharmaceutical products, including online distribution.
- Ministry of Communications and Informatics: regulates issues regarding personal data protection, electronic systems and digital health technologies.
- National Research and Innovation Agency: actively coordinates and supports research and innovation, including efforts in the digital health sector.

- Research partners: among others, Transform Health Indonesia collaborates with research centres, academic institutions and governmental bodies to advance research and innovation in the digital health sector.
- Investors:venture capital firms in recent years have provided funding to digital health startups operating digital platforms.

Law stated - 21 March 2024

Investment climate

2 | How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

The investment landscape for digital health technologies in Indonesia has evolved significantly due to global economic challenges and local responses to the covid-19 pandemic. The pandemic underscored the vital role of the health technology sector in crisis management. Efforts to integrate health technology (health tech) have been evident in collaborations between government bodies and digital platforms, particularly in providing free teleconsultations for covid-19 patients during self-isolation. The Ministry of Health has engaged with various digital platforms, including SehatQ, Halodoc and Vascular Indonesia.

Despite economic pressures, the technology sector, including health tech, continues to develop. Looking forward, the digital health sector is likely to encounter post-pandemic challenges requiring support from various stakeholders. The long-term investment climate for health tech startups is anticipated to remain favourable. Although telemedicine use may decrease post-pandemic, it remains substantially higher than before the pandemic. Several global consulting firms project growth in the Indonesian digital health sector, which is evident from the funding received by digital health platforms.

Law stated - 21 March 2024

Recent deals

3 | What are the most notable recent deals in the digital health sector in your jurisdiction?

There have been several recent significant deals in Indonesia's digital health sector. Notable deals from 2023 and early 2024 include:

- Alodokter, a leading local digital health platform, received US$5.2 million in funding from HL Mando and Beacon Venture Capital.
- Living Lab Ventures introduced the Biomedical Fund in early 2024, targeting investments in various health sectors.
- Good Doctor secured approximately US$10 million in Series A funding led by MDI Ventures and Telkom Indonesia.
- East Ventures announced the US$30 million East Ventures Healthcare Fund focusing on early-stage startups.
- PT Astra Digital Internasional, a subsidiary of PT Astra International Tbk, increased its investment in Halodoc through Series D funding, raising US$100 million.

These developments underline the potential of the digital health industry as it is driven by strategic investments.

Law stated - 21 March 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

Investors looking to acquire a stake in digital health ventures must undertake a comprehensive due diligence process that covers that covers the various key matters and issues, including corporate, licensing, IP and data protection.

In terms of corporate matters, assessing the company's corporate status and regulatory compliance is paramount. To establish a new joint venture with a foreign entity as one of the shareholders, the minimum issued and paid-up capital is 10 billion rupiah. Indonesian law further requires all business lines to be codified in a numerical system known as the Standard Business Classification (KBLI). Specifically, a digital platform company must be registered and subsequently obtain a licence for the KBLI number for commercial web portals, which to date does not carry any foreign ownership restriction.

Scrutinising the digital health venture's licensing compliance involves, among other things, identifying whether it has obtained a valid electronic system provider registration certificate (ie, the certificate required if a business actor intends to operate an electronic system). The investor should also determine whether the digital health venture has undergone or is undergoing a regulatory sandbox on digital health under the jurisdiction of the MOH, and any additional licences required for each of the digital health venture's business activities.

Aside from general corporate matters and licensing, it is prudent for investors to evaluate whether the company has essentially adhered to data protection and cybersecurity provisions in the prevailing laws and regulations. Aside from Indonesian data privacy laws,

the Health Law and the Indonesian Code of Medical Ethics require the data of patients to be kept confidential, subject to several exemptions.

Law stated - 21 March 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

Equity funding (either direct or indirect) is the most common financing structure used by digital health ventures in Indonesia. Generally, digital health ventures, particularly startups, receive such funding from venture capital firms and/or corporations. A foreign entity may also directly invest through capital ownership in digital health ventures in Indonesia, which then would render the venture to be the subsidiary of the foreign entity.

To date, there are no significant government financing or related initiatives by the Indonesian government to support the development of the digital health sector in particular. One of the MOH's initiatives to promote the development of the digital health sector is the issuance of MOH Regulation No. 21 of 2020 on the MOH Strategic Plan for 2020–2024 (as amended) (MOH Reg. 21/2020).Other initiatives include the development of digital technologies for the collection of patient data, the development of telemedicine services, the digitalisation of medical records, and flying healthcare to rural areas.

Law stated - 21 March 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 What principal legislation governs the digital health sector in your jurisdiction?

The following are the pertinent and prevailing legislation governing the digital health sector:

- The Health Law;
- Ministry of Health (MOH) Regulation No. 90 of 2015 regarding the Implementation of Health Services in Health Service Facilities in Remote Areas and Very Remote Areas, which provides that telemedicine is one of the ways to develop health services in remote and very remote areas of Indonesia;
- MOH Reg. 20/2019, which lays out the rights and responsibilities of healthcare facilities, requirements for telemedicine providers, registration obligations for health facilities providing and requesting telemedicine services, and the supervision of telemedicine services by the MOH;
- Food and Drug Authority (BPOM) Regulation No. 8 of 2020 regarding the Supervision of Drugs and Food Distributed Online, as amended by BPOM

Regulation No. 32 of 2020 (BPOM Reg. 8/2020), which aims to protect the public from risks associated with the online distribution of drugs and food;

- MOH Reg. 21/2020, which lays out the strategic plans of the MOH, which include the optimisation of the use of digital health innovations and the development of telemedicine services; and
- MOH Decree No. HK.01.07/MENKES/1280/2023 of 2023 regarding the Development of the Digital Health Innovation Ecosystem Through Regulatory Sandbox (MOH Decree on Regulatory Sandbox), which serves as the basis for the regulatory sandbox to which digital health innovations are subjected.

Law stated - 21 March 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

The notable Indonesian bodies holding jurisdiction over the different facets of the digital health sector are:

- MOH: regulates and oversees health-related policies such as the provision of health services, digital health, including telemedicine services, as well as health information systems;
- BPOM: regulates and oversees issues pertaining to the distribution of medicine and pharmaceutical products, including those distributed online;
- Ministry of Communications and Informatics (MOCI): regulates and oversees issues regarding personal data protection, which includes health data, as well as electronic systems that are commonly used in the digital health sector, especially by telemedicine providers; and
- Ministry of Trade (MOT): regulates and oversees providers of trade through electronic systems, a category which may include Digital Platforms.

Law stated - 21 March 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

Following the issuance of the MOH Decree on Regulatory Sandbox, business actors intending to develop digital health innovations may undergo the regulatory sandbox to be evaluated by the MOH. Upon the MOH's evaluation, the digital health platform will be issued one of the following decisions:

- recommendation;

- conditional recommendation, which means the platform is recommended but needs to be improved within three months; or
- not recommended, which means the platform is rejected without the opportunity for improvement.

Digital Platforms must also obtain the business licences applicable to the web portal business through the Online Single Submission system, which include the Business Identification Number, as well as an electronic system provider (ESP) registration certificate that can be obtained from the MOCI.

If Digital Platform companies or pharmaceutical companies intend to distribute medicine using an electronic system, they must be registered as a Pharmaceutical ESP and obtain a P-ESP certificate from the MOH.

Law stated - 21 March 2024

Soft law and guidance

9 | Is there any notable 'soft' law or guidance governing digital health?

The Minister of Health issued (1) MOH Reg. 21/2020, which serves as a reference for all work units within the MOH in preparing annual planning and implementation of health development programmes, and (2) the Blueprint for Digital Health Transformation Strategy 2024, which lays out the direction and plans for Indonesia's digital health transformation.

The MOH previously issued guidelines in the form of a ministerial decree on the prevention and control of the covid-19 pandemic that acts as a blueprint for healthcare facilities in the provision of digital health services to patients, specifically in the field of telemedicine.

The Indonesian Medical Council (KKI), an autonomous, independent body responsible to the President of the Republic of Indonesia, and the Professional Services Development Council (MPPK) and the Honorary Council for Medical Ethics (MKEK), which are part of the MOH-affiliated Indonesian Doctors Association (IDI), previously issued regulations providing doctors with guidelines for the provision of telemedicine during the covid-19 pandemic. These regulations include:

- KKI Regulation No. 74 of 2020 regarding Clinical Authority and Medical Practice via Telemedicine During the Corona Virus Disease 2019 (COVID-19) Pandemic in Indonesia;
- MPPK Recommendation Letter No. 020/PB/MPPK/05/2020 regarding Telemedicine Services during the COVID-19 Pandemic; and
- MKEK Decree No. 017/PB/K.MKEK/05/2020 regarding Fatwa on Telemedicine Services and Online Consultations, Especially During the covid-19 pandemic.

Law stated - 21 March 2024

Liability regimes

10 What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

To comply with Indonesian law, Digital Platforms typically enter into an agreement with the healthcare facilities and/or healthcare professionals with which they engage and provide terms and conditions (terms) to be agreed upon by platform users. These agreements and terms typically specify the liabilities for the Digital Platforms and the healthcare facilities or healthcare professionals in the provision of services to users, being the patients. As the agreement and terms constitute a contract, the general rule of contracts in Indonesia applies.

Generally, the rule of contracts is governed by the Indonesian Civil Code (ICC), where a contract must satisfy the four basic requirements under the ICC: (1) the parties' consent; (2) the legal capacity of each party to enter a contract; (3) a particular object; and (4) lawful cause. Under the ICC, the party in default is obligated to pay the damages caused by the non-performance of its contractual obligations. Furthermore, as provided under the ICC, liability for a wrongful act is determined on a fault-based assessment, where every wrongful act causing damage to other persons obliges the wrongdoer to provide compensation for such damages.

Additionally, the following points must be taken into account by the parties in allocating liability related to digital health:

- There are no MOH regulations limiting the scope of online medical consultations for doctors as long as they align with ethical obligations in the specific context. Despite the MOH's informal policies, there are no legal barriers to doctors conducting such consultations.
- Alongside legal considerations, medical ethics also play a crucial role. KKI regulation requires doctors to perform necessary medical procedures and diligently assess patients' medical histories, including anamnesis and allergy checks. There is a basic expectation for doctors to conduct informed fact-finding when taking on new patients.
- Certain high-risk, high-cost illnesses require diagnosis confirmation through both the patient's medical history and a physical examination in a formal healthcare setting.
- Healthcare professionals suspected of committing unlawful acts in implementing health services may be subject to criminal sanctions. As for corporate crimes, criminal liability is imposed on corporations, managers with functional positions, parties giving orders to conduct such crimes, parties that exercise control such as majority shareholders and/or beneficial owners of corporations.

The above regulations are silent on the extraterritorial effect of the regulations regarding the cross-border provision of digital health products and services. However, Indonesian data protection laws impose the obligation for data managers to ensure that any cross-border data transfer adheres to the provisions of Law No. 27 of 2022 on Personal Data Protection (PDP Law), including that the recipient country has adequate data protection rules and that the data manager obtain the consent of the concerned data subject.

Law stated - 21 March 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

The Personal Data Protection (PDP) Law stipulates that personal data is the data of individuals that can be directly or indirectly identified, either on their own or in combination with other information (Personal Data). The PDP Law provides three types of personal data relevant to health data, which are:

- health data and information: individual records or information that relates to physical and mental health and/or health services;
- biometric data: data relating to identifiable physical, physiological or behavioural characteristics of an individual, such as facial images or fingerprints. It encompasses unique traits like fingerprint records, retinal scans and DNA samples, requiring careful maintenance and protection; and
- genetic data: any type of data regarding the characteristics of an individual that are inherited or acquired during early prenatal development.

Presently, there are no regulations defining anonymised health data. However, anonymised health data is commonly known as health data that cannot identify an individual, hence it does not constitute personally identifiable information.

In addition to the above, the Health Law and Indonesian Code of Medical Ethics generally stipulate the obligation to maintain the confidentiality of all data related to things identified by healthcare facilities or healthcare professionals in the context of medical treatment and recorded in medical records. There are exemptions to such confidentiality for the purpose of treating a patient, a statutory order, a court request or for public order and safety.

Law stated - 21 March 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

In Indonesia, health data falls under the scope of personal data. Accordingly, the processing of health data must adhere to the lawful basis for personal data processing, which includes:

- the obtainment of an explicit valid consent from the personal data subject;
- the fulfilment of contractual obligations;
- the fulfilment of data controllers' legal obligations;

- the protection of data subjects' vital interests;
- the carrying out of duties in the context of public interest, public services or the exercise of data controllers' lawful authority; and
- the fulfilment of legitimate interests.

The PDP Law classifies the above types of personal data as specific personal data, which is considered to bear a higher risk potential and therefore is subject to a higher degree of protection in comparison to general personal data. When specific personal data is involved in personal data processing, personal data controllers are required to conduct a data protection impact assessment. Furthermore, if the core activities of the personal data controller consist of large-scale processing of specific personal data, it is required to appoint a data protection officer

Finally, the Health Law also provides that health information system organisers are required to guarantee the protection of health data and information, as well as to have a lawful basis for processing health data.

The government is currently planning to issue implementing regulations to the PDP Law. It remains to be seen whether these implementing regulations will affect health data.

Law stated - 21 March 2024

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

Prevailing Indonesian laws and regulations do not recognise the definition of anonymised health data. In any case, anonymised health data is commonly referred to as data that cannot be used to identify certain individuals, hence does not constitute personally identifiable information. Accordingly, the processing of anonymised health data is currently not regulated under the existing regulatory landscape.

Law stated - 21 March 2024

Enforcement

14 | How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

There are presently no regulations governing the treatment of health data specifically in the digital health sector. In any case, as health data falls under the scope of Personal Data, the sanctions within the PDP Law shall apply to non-compliance with the obligations contained therein.

Digital platforms and/or healthcare facilities or healthcare professionals as personal data controllers and/or processors that fail to comply with the obligations stipulated in the PDP

Law may be subject to administrative sanctions in the form of a written warning, temporary suspension of personal data processing activities, deletion or destruction of personal data, and/or administrative fines. Such non-compliance includes failure to conduct a data protection impact assessment or to appoint data protection officer(s).

Specifically, regarding administrative sanctions in the form of administrative fines, the PDP Law stipulates that the violating party may be subject to a maximum fine of 2 per cent of the party's annual income or revenue. These administrative sanctions are to be further regulated by a government regulation. The PDP Law also provides that criminal sanctions include imprisonment and criminal fines. Criminal fines for corporate entities can be imposed up to 10 times the maximum fine for individual offenders.

Law stated - 21 March 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

Presently, there are no regulations specifically governing cybersecurity in digital health offerings. However, the Indonesian government has issued regulations concerning cybersecurity in general and regulations that include cybersecurity-related provisions.

The Indonesian cybersecurity framework is provided under Presidential Regulation No. 47 of 2023 regarding National Cyber Security Strategy and Cyber Crisis Management, which sets out strategic guidelines for governmental institutions and stakeholders in national cybersecurity and cyber crisis management. Although the regulation focuses on measures the government must adopt, it remains relevant for Digital Platforms as the regulation discusses the involvement of electronic system providers (ESP).

Additionally, Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (GR 71/2019) provides that ESPs are obligated to ensure their electronic systems are safe from disturbances, failures and damages, thus requiring Digital Platforms as ESPs to secure their electronic systems.

Law No. 11 of 2008 regarding Information and Electronic Transactions (as amended) (EIT Law) also contains provisions related to cybersecurity, which includes prohibitions regarding the illegal and unlawful:

- access to computers and electronic systems, including violating, breaching, by-passing or penetrating security systems;
- interception of electronic information or documents on computers and electronic systems;
- alteration and transmission of electronic information or documents;
- disruption of electronic systems, including actions that cause electronic systems to not be able to function properly;
- production, sale, procurement for use, importation, distribution, provision, or ownership of:
    -

computer hardware or software that is designed or developed to facilitate prohibited acts stipulated within the EIT Law; and

- computer passwords, access codes and similar items that are designed or developed to facilitate prohibited acts stipulated within the EIT Law.

The above restrictions also apply to parties committing prohibited acts provided within the EIT Law from outside of Indonesian territory towards electronic systems located within the Indonesian jurisdiction.

Law stated - 21 March 2024

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

The use of raw data should adhere to the applicable PDP regulatory framework if such data falls under the scope of personal data that belongs to individual(s) or is identifiable to individual(s). Insofar as the anonymised data do not fall under the definition of personal data, the obligations provided under the PDP Law do not apply to the processing of the data. Pertaining to the output of digital health solutions, if such data falls under the definition of personal data, the processing of such data shall adhere to provisions of the PDP Law.

Law stated - 21 March 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Although the current regulatory framework on patents does not specifically address the patentability of digital health-related inventions, prevailing regulations on patents apply to such inventions. In Indonesia, the protection of patentable inventions is divided into two categories:

- Patents: Inventions that are novel, involve inventive steps, and are industrially applicable.
- Simple patents: Inventions that are novel, enhance or develop existing inventions, have practical uses, and are industrially applicable.

For a patent to be considered novel, the invention must introduce technology distinct from what has been previously disclosed. The element of an inventive step requires that an invention cannot be anticipated by someone possessing expertise in the relevant field.

The requirement that the invention be industrially applicable will be determined by the Directorate General of Intellectual Property (DGIP) when examining the patent registration application, which should elucidate the relevance of the patent and its applicability in an industrial context.

The patentability of digital health-related inventions is determined by whether they may fall under the definition of a patent or a simple patent, and so long as they do not fall under the categories of inventions that cannot be patented. The following are inventions that cannot be patented:

- processes or products that are contrary to applicable laws and regulations, religion, public order or decency;
- methods of examination, care, treatment and/or surgery applied to humans and/or animals;
- theories and methods in the fields of science and mathematics;
- living creatures except microorganisms; or
- biological processes that are essential for producing plants or animals, excluding non-biological processes or microbiological processes.

The current regulatory framework protects inventions but does not explicitly address the issue of employee inventions nor the specific protection of software, algorithms, databases or AI-generated content. The only reference to algorithms is the inclusion of algorithms as an invention that is patentable. Additionally, computer programs and databases may be protected by copyright.

Pertaining to the determination of inventorship and ownership, the Indonesian regulatory framework provides that the employer will be the patent holder of an invention created by their employees during the course of their employment. The employees in question, however, will be recognised as the inventors and such recognition shall be incorporated in the patent registration.

Law stated - 21 March 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

There are no specific application and registration procedures for digital health technology patents. Accordingly, such registration will follow the application and registration procedures that apply to other types of inventions.

To apply for patent rights, parties must file the patent registration to the DGIP of the Ministry of Law and Human Rights via the patent registration webpage. Parties have to submit an application form provided by the DGIP, followed by the payment of the state's non-tax revenue. After filing a patent registration to the DGIP, the following timeline applies:

-

following complete submission of the documents, if the documents are deemed incomplete, the applicant will be able to complete the documents within three months, which may be extendable to six months;

- waiting period for a maximum of 18 months;
- announcement of the completion of the application, with the announcement made a maximum of seven days after the waiting period;
- substantive examination of the application for a maximum of 30 months after the lapse of this period, the result of the application process will be issued; and
- the issuance of certificates within two months.

The above timeline is based on the assumption that the documents submitted are complete and that there are no objections from other parties.

Law stated - 21 March 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Aside from patents, the following IP rights are relevant in the provision of digital health services:

- Trademark: Protects brands and logos that are incorporated by digital health providers. To apply for trademark protection, parties must file a registration via the DGIP's trademark website.
- Copyright: Copyright may protect educational materials, databases and computer programs, among others. Contrary to most IP protection, copyright does not require a registration procedure. However, parties can file for a recordation of the copyright through the DGIP's copyright website.
- Industrial Design: The provision of digital health services may include the utilisation of a graphical user interface (GUI), which may be considered a creation that is subject to the protection of industrial design. The current Indonesian regulatory framework regarding industrial design does not specifically regulate the protection of GUI. Practically, numerous GUI applications have been approved by the DGIP and are subject to the protection of industrial design rights. To secure industrial design rights, parties must apply to the DGIP's industrial design website.
- Trade Secret: Acknowledging the importance of algorithms, data sets and software components in the provision of digital health offerings, such information may be protected as a trade secret so long as it has economic value and is not known to the general public. Trade secrets do not need to be registered or recorded. However, trade secret licences should be recorded on the DGIP's trade secret website.

Law stated - 21 March 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

The licensing of IP rights must consider both legal and commercial implications. From a legal perspective, parties must determine the scope of the licence granted, its limitations, duration, terms of payment and the ownership of the IP.

From a commercial perspective, parties are typically more interested in identifying the target audience or potential customers, the value of IP licensed, and perhaps most importantly, whether the licensing of IP rights will be favourable for the purpose of expanding its market. More specifically for patent holders, the following key considerations should be noted:

- the duration of protection as patents are only protected for 20 years (or 10 years for simple patent);
- whether it would be more strategic to conduct IP licensing or to transfer the patent rights; and
- the financial benefits that licensing IP rights would provide.

Law stated - 21 March 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

The general procedures concerning the enforcement of IP rights also apply to digital health technologies, where the protection of IP rights commonly begins after the registration of IP rights. Under the prevailing laws and regulations, violations of IP rights may be subject to criminal and civil sanctions, including imprisonment, criminal fines, compensation and the cessation of actions that are detrimental to IP owners. Based on publicly available information, there are to date no notable enforcement actions involving digital health technology stakeholders in Indonesia.

Law stated - 21 March 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

The following are the main regulations applicable to the advertising and marketing of digital health products:

- Food and Drug Authority Regulation No. 2 of 2021 regarding Guidelines for Monitoring Drug Advertising: provides the technical details for advertisements for medicines, including that the information contained in advertisements must be objective, complete, not misleading, and should be according to the information contained in the product's distribution permit;
- Ministry of Health (MOH) Regulation No. 1787/MENKES/PER/XII/2010 of 2010 regarding Health Service Advertisements and Publications: provides the provisions governing the advertisement of services by healthcare facilities. Healthcare facilities must ensure that advertisements and/or publications contain accurate information with accurate data based on evidence, and are informative, educational and responsible; and
- Law No. 8 of 1999 regarding Consumer Protection: regulates prohibitions regarding advertisements to protect consumers.

Law stated - 21 March 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

There are currently no specific regulations governing digital health e-commerce platforms. But the following issues regarding e-commerce are applicable to digital health platforms:

- E-commerce activities: e-commerce activities are regulated under MOT Regulation No. 31 of 2023 regarding Business Licensing, Advertising, Guidance and Supervision of Business Actors in Trading Through Electronic Systems and Government Regulation No. 80 of 2019 regarding Trading via Electronic Systems.
- Electronic systems: digital health providers operating their electronic systems will be required to be registered as an electronic system provider (ESP) and are subject to provisions within both GR 71/2019 and MOCI Regulation No. 5 of 2020 regarding Electronic System Providers in the Private Sector, as amended by MOCI Regulation No. 10 of 2021.
- Electronic contracts: electronic contracts, including terms to be agreed by platform users, that are addressed to Indonesian citizens must be formulated in Bahasa Indonesia and adhere to the Indonesian Civil Code. Additionally, electronic contracts must, among other things, include the identity of the parties, objects and specifications, electronic transaction requirements, prices, cancellation procedures, refund or replacement procedures, and electronic transaction settlements.

Law stated - 21 March 2024

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Indonesia's mandatory health insurance programme does not cover digital health products and services. The national healthcare system emphasises reliance on health facilities. However, during the covid-19 pandemic, the Indonesian government collaborated with telemedicine platforms to offer free doctor consultations and medicine delivery for covid-19 patients in self-isolation.

Conversely, several private insurers have offered coverage or reimbursement for the use of digital health products and services, collaborating with existing providers such as Halodoc. Insurers such as AXA Mandiri, Allianz, Prudential, BNI Life, Manulife and Sinarmas have partnered with Halodoc. Additionally, many insurers extend coverage or reimbursement for digital health services to employees under private corporate health insurance plans.

Law stated - 21 March 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

Recent developments in Indonesia's digital health sector include the increase in venture capital investments, which will accelerate the growth of digital health platforms. And the recent amendment of the Health Law means the law now governs telemedicine services, providing a dedicated legal framework and highlighting the sector's growing significance in the healthcare landscape.

The Ministry of Health (MOH) has also established a regulatory scheme to ensure the safety and quality of digital health innovations, emphasising user protection and risk management. With the establishment of this scheme, digital health platforms may have the opportunity to undergo evaluation by the MOH through a regulatory sandbox.

Law stated - 21 March 2024

Winnie Yamashita Rolindrawan winnierolindrawan@ssek.com
Mutiara Kasih Ramadhani mutiararamadhani@ssek.com
Gabriela Eliana gabrielaeliana@ssek.com

SSEK Law Firm

Read more from this firm on Lexology

Japan

Junichi Kondo, **Masayuki Yamanouchi**, **Yuta Oishi**, **Marina Asai**
Anderson Mōri & Tomotsune

Summary

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

Universities and national research institutions, medical institutions, pharmaceutical and medical device manufacturers and other entities are conducting research, development, marketing, promotion, sales and use of healthcare products and services. In the medical devices field, entities from other industries, such as electronic appliance manufacturers, petrochemical manufacturers and IT providers are also active. Partnerships between academic institutions, medical institutions and companies are commonly seen in the research and development stage.

The growth in the digital health market is rapid, and various products and services have been recently launched, but the use of smartphones and applications for medical treatment represents a prominent area of innovation. In June 2020, an application supporting smoking cessation was the first application to be authorised as a medical device, followed by the electrocardiogram application for Apple Watch, which was authorised as a medical device in September 2020.

Law stated - 15 February 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

Against the backdrop of a comprehensive national health insurance system and an ageing population, healthcare costs make up the largest portion of the government's budget deficit. Therefore, the government is focusing on its initiatives to streamline the entire healthcare process, and digital health technologies are expected to play a significant role. Private firms, from the traditional healthcare industry as well as from other areas, are vigorously contributing to the digital health technology business. Foreign investors, however, should pay close attention to potentially applicable medical device regulations, regulations relating to the national health insurance system and recently tightened foreign investment regulations.

Law stated - 15 February 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

In 2019, LINE Corporation, one of the largest social network service providers in Japan, and M3, Inc, the provider of the largest social network service platform exclusively for healthcare professionals in Japan, formed a joint venture, LINE Healthcare. LINE Healthcare provides online, around-the-clock, preliminary health consultation services by licensed physicians. In September 2022, CureApp launched a mobile app to assist physicians' high blood-pressure care. The app offers a six-month programme combining the patient's periodic self-check of their blood pressure and a physician's guidance, which is covered by the national health insurance.

This first authorisation and commercialisation of mobile app as a medical device is followed by several players. Shionogi & Co., Ltd. and SUSMED, Inc are co-promoting SUSMED, Inc's insomnia disorders treatment support app which obtained a marketing authorisation as a medical device in February 2023, and Astellas Pharma Inc. and Roche DC Japan K. K. entered into a partnership agreement in March 2023 to co-develop and commercialise Welldoc, Inc's FDA-cleared app for diabetes treatment in Japan.

Further, an electrocardiogram app and an irregular rhythm notification app installed on Apple Watch were authorised in 2022 and 2023.

Law stated - 15 February 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

If the target company's business involves the manufacturing, marketing or sales of medical devices, an investor should confirm the existence of valid business licences, including:

- a medical device marketing licence;
- a manufacturing licence;
- a sales licence required underthe Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices; and
- the authorisation, certification and registration of each product.

Failure to obtain licences or the required authorisation, certification or registration may lead to penalties and suspension of business, and therefore may have a critical impact on the target company's business.

Intellectual property rights are often essential for the continuation of digital health-related business, so an investor should confirm the status of those rights and the existence of any possible conflict. In addition, due diligence on matters related to employee inventions is necessary. The Patent Act provides that the employer may acquire the patent or patent rights to an employee's invention in accordance with an employment contract or company rules if the invention was created within the scope of the business of the employer and as part of the employee's service. Acquisition of a patent right by an employer requires the provision of a reasonable remuneration or other economic profits to the inventor employee.

If a court finds that the remuneration or profits provided were unreasonable, the employer must provide the deficit, which may have a significant impact on the financial status of the employer. In determining whether the remuneration or profits provided were reasonable, a court will examine, among other things, the negotiations between the employer and employees in adopting the company rules, the disclosure status of those rules, and the hearing status of opinions from the inventor employee. Therefore, an investor should confirm whether the employment contract or company rules stipulate an adequate process for acquiring employee inventions, and whether any past provision of remuneration or profits to inventor employees were completed in accordance with the contract or rules.

Law stated - 15 February 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

The Japan Agency for Medical Research and Development (AMED), an organisation based on the Act of the Japan Agency for Medical Research and Development and governed by the Prime Minister, provides funds for research and development projects in the healthcare sector, including the development of medical devices and systems in the digital health sector. Those funds are typically provided to universities, research institutions and project teams consisting of university or research institutions and private businesses. For example, the AMED provided funds for a clinical trial led by a university of an eye-measuring device and a diagnostic programme for the eye-measuring device.

In addition, several local governments, such as the Tokyo Metropolitan Government, support companies starting businesses in the healthcare sector. However, the recipients of that support are limited to local companies conducting specific businesses (eg, a manufacturing business) within the region or those partnering with those local companies.

Law stated - 15 February 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 What principal legislation governs the digital health sector in your jurisdiction?

There is no specific legislation for the digital health sector. Existing legislation schemes are applied to the digital health products and services as follows.

The Pharmaceuticals Act

A product, which may be either a device or software, that constitutes a medical device pursuant to the Act on Securing Quality, Efficacy and Safety of Products Including Phar

maceuticals and Medical Devices (the Pharmaceuticals Act) will be governed by that Act. A medical device is defined 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.

The Medical Practitioners' Act

Medical diagnosis and treatment are governed by the Medical Practitioners' Act. This Act also covers online medical diagnosis and treatment.

Law stated - 15 February 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

The Ministry of Health, Labour and Welfare (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 concerning 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 (the PMDA), an organisation established under the Law for the Pharmaceuticals and Medical Devices Agency.

Further, the grant 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, are partially delegated to local governments.

Law stated - 15 February 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

If a company's digital health product constitutes a medical device, the company must obtain:

- a marketing licence, manufacturing licence and distributing licence to conduct marketing, manufacturing and distribution of the medical device product; and
-

authorisation, certification or notification for the specific medical device product, according to the statutory classification, which is determined in accordance with the risk that the device would have on the human body in the case of malfunction.

The classification and required procedures for each medical device are as provided in the following table. The classification is harmonised through the International Medical Device Regulators Forum, which succeeded the Global Harmonisation Task Force founded by Japan, the United States, the European Union, Canada and Australia.

Risk	Classification		Requirement
Low	Class I	General medical devices	Notification
Medium	Class II	Controlled medical devices	Authorisation by the PMDA
		Designated controlled medical devices	Certification by accredited certification body
High	Class III, IV	Specially controlled medical devices	Authorisation by the PMDA
		Designated specially controlled medical devices	Certification by accredited certification 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 to the PMDA, regardless of the classification above.

Law stated - 15 February 2024

Soft law and guidance

9 | Is there any notable 'soft' law or guidance governing digital health?

The MHLW and other governmental bodies have issued guidance regarding the digital health sector. Notably, the MHLW issued Guideline on whether Computer Program falls under the Medical Device, which provides a clearer indication of whether certain software constitutes a medical device than is provided in the Act on Securing Quality, Efficacy

and Safety of Products Including Pharmaceuticals and Medical Devices and the ministry ordinance, as well as case studies as to whether Computer Program falls under the Medical Device and database. The guideline states that the question of whether certain software constitutes a medical device should be decided based on, in principle, the purpose of use of such software and the risk of affecting the life and health of a person in the event of software malfunction. Furthermore, the guideline contains examples of software that does and does not constitute medical devices.

Law stated - 15 February 2024

Liability regimes

10 What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

The Civil Code provides that compensation for a breach of an obligation will consist of the damages that would ordinarily arise from that breach. The Civil Code also provides that the intentional or negligent infringement of another person's right constitutes a tort, and that the damages arising from that tort will be compensated. In all cases, damages must have a legally sufficient nexus with the breach or tort to be compensated. Damages may include lost profits and indirect, special or consequential damages, as long as the damages have a legally sufficient nexus to the harm.

In addition, the Product Liability Act provides that a manufacturer or an importer of a product will be held liable for damages arising from the infringement of life, body or property of others that was caused by a defect in the delivered product. Under this Act, a manufacturer or importer will be held liable regardless of whether they acted with negligence, unless the manufacturer or importer establishes that the defect in the product could not have been discovered given the state of scientific or technical knowledge at the time that the product was delivered, or that it was not negligent with respect to the occurrence of a defect in a product that is a component or material of another product that occurred primarily due to the instructions by the other product's manufacturer.

Law stated - 15 February 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

The Act on the Protection of Personal Information defines personal information as information relating to a living individual containing name, date of birth or other descriptions whereby a specific individual may be identified, or information, including individual identification codes (characters, letters, numbers, symbols or other codes that may identify a specific individual, such as fingerprint data processed for fingerprint authentication).

There is no specific data protection and management scheme for health data, and there is no standard definition of 'health data' or 'anonymised health data'. However, 'special care-required personal information' is defined as personal information that may lead to discrimination against, or other disadvantage to, the individual, such as information regarding race, religion, social status, medical records and criminal records. Therefore, health data usually constitutes special care-required personal information.

Further, the term 'anonymously processed information' is defined in the Personal Information Protection Acts 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 (namely, descriptions that could identify an individual because of the uniqueness of the information).

The restrictions on the acquisition, disclosure and use of personal information are substantially eased for anonymously processed information.

Law stated - 15 February 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Disclosure of personal information to a third party requires consent from the data subject, which 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 his or her 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.

Law stated - 15 February 2024

Anonymised health data

13 Is anonymised health data subject to specific regulations or guidelines?

Although disclosure and usage of anonymised personal information are subject to low-level restrictions, explicit consent is 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, so the accumulation of medical information and construction of a database has been difficult.

Therefore, Japan established the Next Generation Medical Infrastructure Act 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 this Act, an authority will examine and authorise entities to be data processing entities that collect, de-identify and provide medical information to third parties (the 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 selects the relevant data, de-identifies it and provides an anonymised data set for a fee.

Additionally, the Next Generation Medical Infrastructure Act was amended in May 2023, and will be in force in 2024. Under the amended Act, medical data can be provided to the Authorised Pseudonymized Medical Information Preparer through the opt-out procedure. Pseudonymized Medical Information created by the preparer can be used by users authorised under the amended act.

Law stated - 15 February 2024

Enforcement

14 How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

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, collects reports and conducts on-site inspections, and makes recommendations and orders, etc, regarding legal violations. Japan does not have a long history of using digital healthcare technology, so no notable regulatory or private enforcement actions have been published.

Law stated - 15 February 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

The Ministry of Health, Labour and Welfare (MHLW), the Ministry of Economy, Trade and Industry, and the Ministry of Internal Affairs and Communications have introduced two guidelines concerning the management of health information (the Medical Information Guidelines).

The Safety Management Guideline for Providers of Information Systems and Services that Handle Medical Information (version 1.1) contains guidance for providers that supply medical information systems and resources and services necessary for those medical information systems, and providers that receive medical information from medical institutions based on the instructions of patients, etc, including providers of applications (ASP/SaaS), platforms, infrastructure (IaaS) and communication lines (the Providers). This guideline is focused on information created or recorded by healthcare providers. The guideline requires Providers to either (1) obtain a privacy mark, an information security management system certificate or other designated certificates, or (2) be audited by a qualified external auditor. 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.

The Guideline on Safety Management of Medical Information System (version 6) contains guidance for medical institutions and applies to information created or recorded by healthcare providers. The guideline requires the preparation of internal standard operating procedures for safety management, the appointment of medical information system safety manager and planning and administration manager, the implementation of staff training and incident reporting and responding standards, as well as measures to prevent eavesdropping, falsification or security breaches when exchanging information with outside parties via the network. The guideline contains requirements for the electronic storage of medical information.

Japanese courts have been reluctant to award large amounts of damages relating to claims of leakage of personal information, with amounts generally ranging from ¥3,000 to ¥30,000 per person. There is, however, a notable case in which a nurse disclosed information to her husband regarding a terminal patient's medical state. The court found that the nurse had repeatedly disclosed similar information, and concluded that the hospital had failed to properly supervise the nurse, ordering the hospital to pay ¥1.1 million to the bereaved family.

Law stated - 15 February 2024

Best practices and practical tips

16 | What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

In practice, the Medical Information Guidelines require that medical information be stored in Japan. However, the purpose of this requirement is to facilitate the MHLW's supervision and audit of medical institutions, so copies of medical information may be stored overseas

if a complete copy of the information is also stored within Japan. This restriction is only applicable to information collected by medical institutions, rather than by other parties.

Law stated - 15 February 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Software may be protected by a patent as either a product or a process if:

- the software controls an apparatus or processes information based on the technical properties of an object; or
- the software uses hardware resources to construct a specific information processing system or an operational method for the system.

Mathematical algorithms, databases and AI-generated content are not patentable. Additionally, methods of surgery, therapy or diagnosis are not patentable.

The right to obtain a patent may be assigned from an employee to an employer, or may be acquired by the employer in the first instance in accordance with rules established by the employer. In those cases, the employer must compensate the employee in accordance with the employer's rules. If a court finds that the compensation was unreasonable based on a lack of due process in the establishment and circulation of the rules or in the compensation process, it may determine the amount of the compensation after considering various factors, including the profits arising from the exclusive right to the invention and the employer's own contribution to the invention.

Law stated - 15 February 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

There is no special patent application and registration process for digital health technologies. To obtain a patent, an applicant must first file an application with the Japan Patent Office. Within three years of the application date, the applicant must file a request for examination to initiate the substantive examination of the application. Then, an examiner will render a decision to grant a patent or will notify the applicant of the reasons for refusal of a patent. The applicant will be given an opportunity to amend the claims to overcome the reasons for refusal, and to submit a written document arguing that a patent should be granted. If the examiner finds that the reasons for refusal have not been overcome, the examiner will decide upon refusal. This decision may be appealed to the board of patent

appeals. An unfavourable decision by the board is appealable to the Intellectual Property High Court (IPHC), and judgments rendered by the IPHC are appealable to the Supreme Court.

The Japan Patent Office's website discloses a schedule of official fees.

Law stated - 15 February 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Computer programs that are incorporated into digital healthcare products are copyrightable. An author of a computer program may obtain a copyright without any formal process. An employer may originally obtain, as an author, the copyright for a computer program invented by its employee in the course of his or her duty and at the initiative of the employer, unless otherwise agreed to, or stipulated in, the employer's rules. An author also retains moral rights, which consist of a right to make a work public, a right of attribution and a right to integrity. Moral rights are not transferrable by agreement. Thus, when obtaining a copyright from an author, an assignee should ask for a written agreement from the author not to exercise his or her moral rights.

A database may be protected as a trade secret if it is useful for business, controlled as confidential and not publicly known. Further, a database may be protected as 'shared data with limited access' even when it is open to the public if the data constitutes technical or business information that is managed and accumulated to a reasonable degree by electronic or magnetic means and is provided to specific people on a regular basis.

Law stated - 15 February 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

Digital health products commonly generate a significant amount of data. Therefore, parties to an agreement should decide how to handle generated data, including whether a licensor or licensee may use or modify such data, whether they may disclose data, and what IP rights, if any, the licensor or licensee may obtain.

Further, data generated by digital health products may include personal or medical information. A licensor and licensee must acknowledge that such information must be processed or stored in accordance with the Act on the Protection of Personal Information.

Additionally, digital health products, including computer programs, may be classified as medical devices. If a licensor provides those products directly to a licensee, or if the licensee plans to sell those products, the licensor or licensee must obtain the licences required by

the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices.

Law stated - 15 February 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

IP rights are generally enforced through infringement lawsuits filed by IP owners seeking damages or injunctive relief. Damages are typically lost profits, profits of accused infringers or a reasonable royalty. A court may issue an injunction if it finds that the defendant has committed, or is likely to commit, infringing activities. The Japanese court system has three levels: district courts, high courts and the Supreme Court.

IP owners may also seek a preliminary injunction. A court may issue a preliminary injunction if it finds a prima facie case of infringement and the likelihood of irreparable harm to the petitioner. When issuing a preliminary injunction order, a court will require the petitioner to post a bond that could compensate the accused infringer for damages if the court finds that the preliminary injunction should not have been granted.

Further, IP owners may request border enforcement of IP rights by filing a complaint with a customs office. Finally, the Japanese penal system provides that an infringer may be subject to imprisonment or a fine, but the imposition of a criminal punishment is rare.

We are unaware of any notable enforcement actions involving digital health technologies.

Law stated - 15 February 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

There are no specific rules or restrictions governing the advertising and marketing of digital health products and services. However, the following laws may apply.

The Pharmaceuticals Act and related guidelines

If a product or service constitutes a medical device, advertisement and marketing for that product or service will be regulated by the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices (the Pharmaceuticals Act). Advertisement of an unauthorised medical device or an off-label use of an authorised medical device

is strictly prohibited. The Ministry of Health, Labour and Welfare's Guideline on Adequate Advertisement of Pharmaceuticals, etc, provides detailed rules relating to the advertisement of medical devices, including a prohibition on advertising comparisons with other manufacturers' products.

The Act Against Unjustifiable Premiums and Misleading Representations

The Act Against Unjustifiable Premiums and Misleading Representations governs all consumer products, including digital health products, and services marketed towards consumers. Medical devices and other products governed by the Pharmaceuticals Act are also governed by this Act. 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 terms of a product or service that could be misunderstood to be significantly more advantageous than the terms of the actual product or service.

The Medical Care Act

The Medical Care Act restricts advertisements by medical institutions. The Act prohibits false or extravagant advertisements, as well as advertisements that include a patient's experience or 'before' and 'after' photographs. This restriction applies to advertisements regarding the treatment or service offered at a hospital or clinic using a digital health product or service.

Law stated - 15 February 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

The Civil Code provides that an agreement is formed upon the manifestation of one party's intent to accept another party's offer to enter into an agreement, and does not require any formalities for effectuation of agreements, except in a few instances that are not relevant here. Thus, an agreement made orally or through digital communication is effective, and there are no specific conditions for the effectuation of electronic contracts.

The Act on Specified Commercial Transactions regulates online sales in general, including sales of digital health products or services. This Act provides, for example, that:

- a consumer may cancel his or her purchase within eight days from the receipt of the product, or the receipt of the statutory document relating to the purchase of services, unless the advertisement provides a special policy condition prescribing otherwise;
- the price, timing of payment, means of payment, time of delivery and other conditions concerning the sale must be indicated in the advertisement;
- misleading advertisements are prohibited; and

- sending email advertising to a person who has not given consent is prohibited.

In addition, if the service provider processes its customers' payments, rather than relying on other payment means such as another issuer's credit card, the service provider may be considered to be a funds transfer service provider pursuant tothe Payment Services Act and, therefore, must register with the Prime Minister.

Law stated - 15 February 2024

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

In Japan, all residents are covered by national health insurance, including the employee insurance system, the national health insurance system or the medical insurance system for the elderly. Patients receive treatment at a medical institution and pay a portion (10 to 30 per cent) of the cost of treatment at that medical institution. The remaining cost is billed to the assessment and payment agency, which reimburses the medical institutions from the insurance premiums collected from the insured by the health insurance association, with the government covering any deficit.

The Ministry of Health, Labour and Welfare ordinance prescribes the coverage by the national health insurance system of 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, 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.

Law stated - 15 February 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

The Foreign Exchange and Foreign Trade Act regulates foreign exchange transactions, foreign trades and inbound and outbound investment. Typically, an inbound investment by a foreign investor, such as an acquisition of equity in a Japanese company, must be the subject of a post facto report to the Bank of Japan. However, inbound investment into certain listed industries requires prior notification followed by a 30-day waiting period, during which the government may issue an order to stop or change the investment.

As a result of the amendment to the Act and the addition of the specially controlled medical device (Class IV) manufacturing business to the core business list by the Minister of Finance in June 2020, a 30-day prior notification is required for certain investments into the specially controlled medical device (Class IV) manufacturing business in Japan as provided in the following table.

	Acquisition of shares of less than 1 per cent	Acquisition of shares of 1 per cent or more, but less than 10 per cent	Acquisition of shares of 10 per cent or more
No notification required	Prior notification is required if any of the following items are met: • the investor appoints him or herself or any person related to him or her as the director or the auditor of the issuing company; • the investor, either by him or herself or through another shareholder, proposes important business matters concerning the designated business,	Prior notification required	

	such as business transfer, to the shareholders' meeting of the issuing company; • the investor accesses undisclosed technical information pertaining to businesses in the designated industries; • the investor attends, or causes any person he or she has designated to attend, the board of directors' meeting or a meeting of any other important decision-making committee of the issuing company; or • the investor makes a proposal in writing or in an electromagnetic record to the board of directors or other			

	important decision-making committee of the issuing company.		
Prior notification required	Prior notification required	Prior notification required	

Law stated - 15 February 2024

ANDERSON MŌRI & TOMOTSUNE

Junichi Kondo junichi.kondo@amt-law.com
Masayuki Yamanouchi masayuki.yamanouchi@amt-law.com
Yuta Oishi yuta.oishi@amt-law.com
Marina Asai marina.asai@amt-law.com

Anderson M ri & Tomotsune

Mexico

Bernardo Martinez-Negrete, **Lisandro Herrera**
Galicia Abogados SC

Summary

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

The key players active in the development of digital health technologies in Mexico are start-ups (mainly tech companies), healthcare providers such as hospitals, academic institutions and investors. The principal areas of innovation are:

- medical software;
- healthcare apps;
- artificial intelligence analysing clinical lab tests and research;
- telemedicine; and
- electronic health records.

Law stated - 31 January 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

The digital health market has been growing steadily in Mexico in the past couple of years. It has been positively affected by the intense growth of the information technologies market in the country, which (with an output of US$15.5 billion) grew at a rate of 9 per cent during the first quarter of 2020. One challenge is the lack of regulation for several digital health technologies; however, a regulation proposal is currently being discussed in Mexico's Congress.

Law stated - 31 January 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

Despite a lack of enthusiasm from the federal government when it comes to digital health matters, local state authorities have been open to digital health technologies. This has allowed the implementation of digital health systems in various states through public–private partnerships and other schemes where the private investor is responsible for the development and management of the infrastructure and the state is responsible for bringing patients into the hospital. For example, some financial institutions have created a healthcare services provider for the beneficiaries of insurance companies in selected

hospitals and for supplying medicine prescribed by doctors through pharmacies. In such a system, the healthcare services provider, hospitals, insurance companies and pharmacies are all linked, allowing the patient to have a remote appointment with their doctor, who can prescribe medicine digitally. The prescription can be obtained online from a pharmacy or by using a QR code, and the payment by insurance companies is done remotely.

Another example is the implementation of digital technology in operation rooms, where private investors develop the technology – including software and health inputs (such as surgical medical instruments and medicine) – to help with various operations in government facilities. The government enters into a contract for the services with the provider for a certain number of years, and at the contract's expiration the government has the option to buy the technology.

Law stated - 31 January 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

The first and most important matter is understanding how the products or services of a digital health venture are classified in Mexico. This will determine the requirements (eg, labelling, advertising) and authorisations (eg, marketing authorisations, operation notice) required for the business to operate legally. Another step is verifying that the services or products comply with the Official Mexican Standards or NOMs specified for that kind of service or product (ie, the fulfilment of the Mexican regulation regarding operation rooms and hospital equipment, among others).

Furthermore, it must be determined whether the digital health product or service is intended for public or private markets, as specific requirements may apply to a public-market product.

Law stated - 31 January 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

It is uncommon to receive government financing for digital health ventures; however, some local governments have been open to the implementation of digital health services through public–private partnerships and other schemes, where the private investor is responsible for the development and management of the infrastructure and technology, and the state is responsible for bringing patients into the hospital. The most common financing structure used in digital health ventures is private investment. A large venture capital market in Mexico is focused on technology investments, including digital health (in 2021, technology investments were above US$1 billion). These venture capital investments are often minority equity positions (from 20 per cent

to 30 per cent) and funded through a mix of equity and debt (by local commercial banks and other financial institutions).

Law stated - 31 January 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 | What principal legislation governs the digital health sector in your jurisdiction?

Currently, there is no principal legislation concerning digital health products or services. Such products or services tend to be indirectly regulated under various legislations and standards. For example, the General Health Law contains provisions regarding the use of information and communication technologies in health matters and electronic medical records. The Healthcare Services Regulation likewise contains a provision on digital prescriptions with a focus on the requirements for them to be issued, but it is silent on the issuance of such prescription through digital channels.

In principle, digital products and services must comply with the general regulation applicable to similar products and services that are marketed or offered in the traditional way. These are governed by the General Health Law, the Health Input Regulations, the Healthcare Services Regulation and several Official Mexican Standards, depending on the service or product.

A case worth mentioning is the software as a medical device. The 'Official Mexican Standard NOM-241-SSA1-2021, Good practices for the manufacturing of medical devices', published on 20 December 2021 and coming into force on 21 June 2023, is the first legal provision in Mexico that regulates software as a medical device. Accordingly, software is considered a medical device so long as it:

- is used for one or more medical purposes;
- does not need to be part of a hardware to fulfil its intended purpose;
- can run on general computing platforms; and
- can be used alone or in combination with other products (eg, as a module or other medical devices).

If software (including a mobile application) meets the above criteria it will be considered a medical device, while software that only runs on a specific physical medical device is excluded from such classification and will not require registration to be marketed within the Mexican territory.

There are several initiatives underway to amend the legal framework and regulate digital health. Some are focused on electronic clinical records and digital prescriptions; others place a broader focus on digital health as an ecosystem – these are still pending approval by Congress.

Law stated - 31 January 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

The Ministry of Health is the regulatory and enforcement body for the digital health sector through the Federal Commission for the Protection against Sanitary Risks. The latter entity is in charge of protecting the population against health risks caused by the use and consumption of goods, services and other health-related products.

Additionally, in terms of prices and commercial matters, the Ministry of Economy has jurisdiction over the digital health sector through the Federal Consumer Protection Agency, a body in charge of protecting and promoting consumer rights.

Law stated - 31 January 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

In general, digital health products are mostly classified as medical devices, in which case they must secure a marketing authorisation to become commercialised in Mexico. If a product is manufactured domestically, the facility where the manufacturing takes place must secure a sanitary licence and appoint a sanitary responsible person. However, if the product is manufactured abroad, the warehouse within the Mexican territory where the products are stored must have an operation notice and a sanitary responsible person. In addition to a marketing authorisation, an imported product requires an import permit to enter the country.

In relation to services to be rendered through digital technologies, for the time being there is no specific regulation other than the usual laws applicable to medical services (whenever such a service is performed digitally).

Medical software is not currently classified as a device and, therefore, does not require a marketing authorisation nor an import permit for its commercialisation in Mexico. Software that is necessary in the operation of a medical equipment is considered a part of the device; although the software itself does not require a marketing authorisation, it is included in the marketing authorisation of the medical equipment it runs on. As of July 2023, however, software may be classified as a medical device if it:

- is used for one or more medical purposes;
- does not need to be part of medical hardware to fulfil its intended purpose;
- is capable of running on general computing platforms; and
- can be used alone or in combination with other products (eg, as a module or other medical devices).

Software as a medical device will need to function accurately, completely and according to its design. Therefore, marketing authorisation for software will be needed, though the requirements have not yet been published.

Law stated - 31 January 2024

Soft law and guidance

9 | Is there any notable 'soft' law or guidance governing digital health?

In 2014, the National Center for Health Technology Excellence (CENETEC) issued guidelines on telehealth, telemedicine and the long-distance training of healthcare professionals. These guidelines are not compulsory, are quite broad and have not been properly publicised, so they are barely known and have not been updated since their publication in 2014. The National Health System (the Mexican Social Security Institute for private employees) published its own guidelines on telehealth and telemedicine that are applicable in 12 hospitals in the states of Baja California, Baja California Sur, Sonora, Sinaloa, Nayarit, Jalisco, Colima and Michoacán.

In the context of interoperability, some NGOs have been active in the adoption of international standards for the transfer of clinical data Health Level Seven (HL7).

Law stated - 31 January 2024

Liability regimes

10 | What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

The key liability regimes applicable to health products are civil and administrative. Civil liability is based on damages caused to someone or something by the use of technology or services (malpractice). Conversely, administrative liability does not seek to compensate the damage to the victim but to sanction improper conduct.

In the case of civil liability, any injured or harmed consumer has the right to be compensated for damages caused by the goods or services sold, either as a consequence of:

- contract liability, based on the lack of conformity of the goods or services;
- extra-contractual (tort) liability; and
- strict liability, where there is no need for a wrongful or illicit action or omission to have occurred.

Besides, under Mexican procedural law, a group of at least 30 persons can file a class action to claim damages.

Administrative liability can be determined by the Federal Commission for the Protection against Sanitary Risks (based on a violation of the General Health Law by any act, service

or product that jeopardises public health in any sense), and by the Federal Consumer Protection Agency in charge of protecting and promoting consumer rights. In both cases, the sanctions are remarkably similar and include fines, product seizure, service ban and facility closure.

Cross-border digital health products and services need to comply with similar requirements as those applicable to local products and services; however, there is a practical problem when trying to enforce these rights against a company or a person that does not have an address or a legal representative in Mexico. In both civil and administrative liability, the person responsible for the product or service will be notified and must appear before the Mexican authorities to be held responsible.

Law stated - 31 January 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

Under the Official Mexican Standard NOM-004-SSA3-2012, health data is defined as the patient's unique set of information and personal data held by a medical care establishment, whether public or private, which consists of written, graphic, imaging, electronic, magnetic, electromagnetic, optical, magneto-optical and any other type of document based on which healthcare professionals create records, annotations and certifications corresponding to their intervention in the patient's medical care, in compliance with the applicable legal provisions. Mexican law is silent on anonymised health data.

Law stated - 31 January 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Yes, the level of protection afforded to health-related data in Mexico is greater than any other personal data, as it is regarded as sensitive personal data under the Federal Law for the Protection of Personal Data Held by Private Parties. Sensitive personal data is any personal data that, if misused, could lead to discrimination or cause grave danger to the data owner. As a general rule, all processing of personal data is subject to the owner's consent, expressed in writing.

Besides, databases containing sensitive personal data are only allowed to exist when their legitimate and specific purposes are justified by the responsible party, according to the latter's activities or purposes, and reasonable efforts must be made to limit the processing period to the minimum necessary.

A breach of data protection laws can result in significant fines that range from approximately US$450 to US$1.4 million, depending on:

- the nature of the data;
- the intentional nature of the action or omission constituting the violation; and
- the financial position of the data controller.

Moreover, a violation of provisions concerning sensitive personal data (eg, health data) results in sanctions and penalties. Compromising the security of databases, premises, computer programs and equipment, when attributable to the data controller, is considered a criminal offence that may result in imprisonment for up to three or five years, or twice as much if the offence involves unlawful treatment of sensitive personal data.

Law stated - 31 January 2024

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

No, anonymised health data is excluded from the scope of data protection laws and regulations in Mexico, as such data cannot lead to the identification of a person.

Law stated - 31 January 2024

Enforcement

14 | How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The National Institute for Transparency, Access to Information and Protection of Personal Data (INAI) is the authority in charge of granting access to public information and protecting personal data. INAI is constantly monitoring the operation of the responsible parties and that the collection and treatment of personal data are conducted according to legal provisions, especially those related to sensitive personal data that tend to have stricter requirements.

We are aware that INAI has been reviewing closely those parties in charge of handling sensitive personal health data, and has imposed elevated fines on parties responsible for lack of compliance with data protection legislation. However, from the available information, it is not possible to determine if any of these sanctions were imposed because of the use of digital health technologies.

Law stated - 31 January 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

There are no specific laws on cybersecurity. However, the personal data protection legal framework requires data controllers and processors to put in place adequate technological security measures taking into consideration:

- the nature of the personal data subject to processing;
- the vulnerability of the processing system; and
- the technological developments in the market.

Such security measures must be reviewed and updated regularly. Cyberattacks, hacking, virus infection and other cybercrimes constitute punishable criminal offences pursuant to the Federal Criminal Code, punishable by imprisonment for up to 12 years.

Although there is no specific cybersecurity law in place, in April 2023 a bill for the Federal Cybersecurity Law was presented in Congress, and such draft proposes to create a legal framework pursuant to which public entities and private parties shall be obligated to perform different actions to mitigate, prevent and fight cyberthreats or cybersecurity attacks that could affect the confidentiality, personal data, integrity and availability of information. This bill of law is expected to be discussed throughout 2024.

Law stated - 31 January 2024

Best practices and practical tips

16 | What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Under the data protection laws, data controllers are accountable for complying with legal principles and obligations, including implementing appropriate security measures to protect data against loss, theft and unauthorised use or access. Therefore, it is advisable that any processing of raw health data is preceded by a privacy notice in Spanish that is compliant with data protection legislation and that comprehensively describes the purpose of the process and is updated regularly. The express consent of the owners of the health data must be obtained and kept safe for the duration the data is handled, as the authority may request such information.

In the case of anonymised data, as the owner cannot be identified, it does not fall within the scope of data protection provisions. Therefore, its use, share and any other relevant activity constitutes a commercial decision.

Law stated - 31 January 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Inventions in all technology fields can be patented if they are:

- new and not in the state of the art – that is, technical knowledge made accessible to the public by any means of dissemination in the country or abroad;
- the result of an inventive activity – a creative process whose results are not deduced from the state of the art in a way that is obvious or evident to a technician in the field; and
- are susceptible of industrial application – the possibility that an invention can be produced or used in any branch of economic activity, for the purposes described in the application.

In Mexico, databases, algorithms, software and any other written technology cannot be protected by a patent. These works are protected under the Federal Copyright Law, according to which protection is not required for registration before the competent authority and is not subject to any formality whatsoever; therefore, once the work is fixed on a material support (regardless of its merit, purpose or mode of expression) it will be protected. However, for the copyright to be exercised before a third party, it must be registered with the National Institute of Copyright.

In terms of the Federal Labor Law, employees are entitled to appear as authors of the inventions made for their employer, but the employer owns the inventions and has the right to exploit the patents. Further, employees have the right to receive complementary compensation when the relevance of the invention and the benefits gained by the employer are disproportionate to their salary. Such compensation can be regulated by an agreement between the employer and the employee, which is customary practice in Mexico.

Law stated - 31 January 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

The patent application procedure does not distinguish a digital health technology from any other invention, so they follow the same procedure. The inventor, their successor or legal representatives may apply for a patent, which must comply with all required information and documentation. The application can be filed for a specific invention or a set of related inventions that conform to a unique inventive concept. The Mexican Patent and Trademark Office will first verify that all the requirements are met and, if the recognition of a priority is claimed by the applicant, an 18-month term must pass for its prior publication, which will make the patent application public. Afterwards, the authority will conduct a final verification to determine if the requirements are met, and if the information submitted is not enough

to allow compliance with the legal and technical requirements, additional information will be requested from the applicant to be filed within a two-month period. Once all the legal and technical requirements are met, the authority issues a patent title, granting the holder a 20-year term for exclusive exploitation. The patent title will be published in the official gazette and become enforceable to third parties.

Law stated - 31 January 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

In Mexico, the code of software, databases, algorithms and any other written invention is considered among 'works' and protected through copyright. These kinds of inventions do not require registration or recognition by the copyright authority, as they will be protected once they are fixed on material support. Nonetheless, to enforce copyright before a third party, a certificate from the copyright authority must be secured to increase chances of success.

Law stated - 31 January 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

If a digital health technology is patented, the following considerations must be respected when licensing IP rights:

- the licence must be granted in a written agreement including information on the parties;
- the IP right to be licensed (commercialisation, prosecution, infringement action, etc);
- the term of the agreement and whether it is exclusive or not; and
- the amount to be paid for the licence (or reference that it is a free licence).

Such agreement must be submitted before the Mexican Patent and Trademark Office through a free writ by any of the parties involved in the licensing of the IP right to become effective vis-á-vis third parties.

Concerning software, algorithms, databases and any work protected by copyright, licensing must be compensated and subject to a specific time. The licence can be exclusive or not, and it must be recorded at the National Institute of Copyright to be enforceable on third parties.

Law stated - 31 January 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

IP provisions in Mexico do not include a specific procedure for the enforcement of digital health technologies IP rights. The regular enforcement procedures are observed when enforcing IP rights in digital health technologies. First, an infringement procedure must be initiated before the Mexican Patent and Trademark Office, in which the reimbursement of the royalties earned from the exploitation of an IP right may be imposed on the offending party. The interested party must present all relevant evidence to support the action. The final resolution issued by the Mexican Patent and Trademark Office can be challenged through a nullity claim that must be filed before the Federal Court of Administrative Justice. The court's ruling can likewise be reviewed through an amparo action, which must be filed before the circuit courts whose ruling is final and binding.

Regarding software, algorithms, databases and any work protected by a copyright, an infringement in commerce-related matters can be initiated before the Mexican Patent and Trademark Office. The plaintiff must offer all available evidence that will support its claim, and the final resolution of this procedure can be challenged as referred to above and will follow the same path.

No relevant enforcement action involving digital health technologies has come to our attention so far.

Law stated - 31 January 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

Digital health products classified as medical devices are subject to strict advertising and marketing regulations. The marketing of a digital medical device requires authorisation; however, there is no regulation on the availability of the product to patients, which means that in principle anyone can access it without restriction.

The advertising of a medical device strictly follows the characteristics provided under the marketing authorisation, and the latter determines if advertising can be aimed at the public or healthcare professionals only. If advertising is aimed at the public, it must:

- be clear, concise and easily understandable by its target audience;
- contribute (using claims) to hygiene education; and
-

include precautionary messages (when the use or consumption of the product may present a health risk).

Before advertising a medical device, a permit must be secured from the Federal Commission for the Protection against Sanitary Risks if it is aimed at the public, or an advertising notice must be submitted before the same sanitary authority if advertising is aimed at healthcare professionals.

On the other hand, the rendering of a medical service is subject to submitting an operation notice that provides the location of the facility and the appointment of the sanitary responsible person, who verifies that the services are rendered in line with applicable technical and legal provisions.

The advertising of medical services (regardless of whether they are offered through digital health technology) must inform the public about the type, characteristics and purpose of the services, including the modalities of access. All medical services to be advertised must have a permit issued by the Federal Commission for the Protection against Sanitary Risks.

Additionally, according to the Federal Consumer Protection Law, the advertising or offering of information about a product or service related to digital health technology and disseminated by any means or media must be truthful, verifiable, clear and free of texts, dialogues, sounds, images, brands, denominations of origin and other descriptions that are misleading or abusive. Misleading or abusive information or advertising is understood as that which is inaccurate, false, exaggerated, partial, contrived or biased.

Law stated - 31 January 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

There are no specific e-commerce rules for digital health offerings, but the general e-commerce rules apply (ie, all information on the offering must be truthful, verifiable, not misleading or abusive, and must not confuse the consumer). The terms and conditions of the use of the e-commerce technology must be presented to the consumer or patient in clear and understandable language and must be accepted by them before they use the technology. Moreover, if the e-commerce offering requires the user to include health data (ie, sensitive personal data), a privacy notice must be displayed explaining how the information will be used and treated, allowing the user to grant written and express consent through their electronic signature or any other authentication mechanism.

Law stated - 31 January 2024

PAYMENT AND REIMBURSEMENT

Coverage

24

Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Telehealth and telemedicine are covered by some members of the National Health System, such as the Mexican Social Security Institute (IMSS), the Institute for Social Security and Services for State Workers and other local public health providers. For example, IMSS has a telemedicine programme in 12 hospitals across Baja California, Baja California Sur, Sonora, Sinaloa, Nayarit, Jalisco, Colima and Michoacán. Long-distance learning programmes have also been implemented at the national level by IMSS.

Some private insurers have developed their own telemedicine and telehealth systems to support their beneficiaries; this has been done in collaboration with hospitals, doctors and pharmacy chains.

With respect to hospitals, The National Healthcare System does not work as a reimbursement system of out-of-pocket expenses, but rather as a system where the hospital is obligated to supply medicines or perform services. Patients who receive medical services through private hospitals or doctors may be reimbursed for their out-of-pocket expenses through private insurers.

Law stated - 31 January 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

The most relevant recent development is the 'Official Mexican Standard NOM-241-SSA1-2021, Good practices for the manufacturing of medical devices', published on 20 December 2021 and came into force on 21 June 2023, which regulates software as a medical device. Prior to the enforcement of this standard, software was not classified as a medical device because of its nature, features and use, and such products do not require any additional authorisations for commercialisation (ie, marketing authorisation).

It is worth noting, as a significant development impacting digital health technologies, the fact that Congress is discussing several initiatives to regulate digital health to bring more certainty to the market of products and services related to digital health technologies, as well as the legal and technical requirements these should meet.

Law stated - 31 January 2024

Bernardo Martinez-Negrete bmartineznegrete@galicia.com.mx
Lisandro Herrera lherrera@galicia.com.mx

Galicia Abogados SC

Read more from this firm on Lexology

Singapore

Erwan Barre, **Wun Rizwi**
RHTLaw Asia LLP

Summary

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

There are key players in the different sectors of the digital health market in Singapore. In the government sector, the key players are the Ministry of Health (MOH), MOH Holdings, Office for Healthcare Transformation, National Research Foundation, and Singapore Economic Development Board. The key players in relation to healthcare providers are the National University Health System, National Healthcare Group and Singapore Health Services. The key research partners are the Agency for Science, Technology and Research (A*STAR) and Health Technologies Consortium.

The most prominent areas of innovation are artificial intelligence, telehealth and telemedicine, mobile health (eg, mobile applications and wearable devices), data analytics and digitised and integrated healthcare systems (such as the National Electronic Health Record, which collects patients' health records, and the HealthHub App, which is a national digital healthcare platform).

Law stated - 15 January 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

Medical technology investments and innovations have been a popular focus in the healthcare industry in Singapore given the rapid growth of digital health technology and healthcare research and development. Singapore is an attractive business hub for healthcare innovations with the majority of the population more tech-savvy and receptive to digital health innovations than the more hesitant older population.

The covid-19 pandemic created a surge in demand for digital health products and services, which, in turn, catalysed investments in digital health and across the healthcare industry. As such, the adoption of digital healthcare was greatly accelerated. This was an unprecedented opportunity that shifted the default care model to digital health technologies and virtual services; bringing hospitals to people's homes and increasing accessibility of an individual's health information and records. The digital demand in Singapore presents great opportunity for businesses to ensure high-quality digital services and to introduce digital healthcare solutions that are more effective and convenient.

Moreover, while healthtech startups in Southeast Asia have been finding difficulty in obtaining funding amid economic and geopolitical challenges, from 2020 through September 2023, Singapore had secured 67 per cent of the region's total and raised funds accounting for 80 per cent of the total healthtech funding in Southeast Asia. Singapore has been making steadfast progress in healthcare digitalisation and fortified its position as the epicentre of healthtech investments in the region.

Law stated - 15 January 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

In November 2022, DocDoc, the world's first patient intelligence company, announced a pan-Asia collaboration to offer its health insurance solutions to clients of Aon, an insurance broker, via insurance partners starting with Singapore. The solutions are powered by DocDoc's AI engine 'HOPE' and will empower employees with the personalised information required to make informed decisions across one of Asia's largest and most data-rich doctor networks.

In November 2022, a digital health platform in Singapore, Speedoc, raised S$28million in pre-Series B round funding, which will be used to scale up Speedoc's virtual hospital model. Speedoc is a virtual clinic that provides a range of mobile home care services, including teleconsultations, onsite doctor and nurse visits, virtual hospital wards and ambulance-hailing services. WhiteCoat, a Singapore-headquartered telehealth services provider, which intended to raise US$25 million, had in 2023 closed a tranche of its Series B fundraising round to expand to Indonesia, Vietnam, and Malaysia. WhiteCoat is also a digital health platform that provides services including but not limited to teleconsultation and in-person consultation services with doctors, specialists and allied healthcare professionals.

In March 2023, Temasek-backed SeaTown Holdings had invested S$150 million in Singapore-based medical group Foundation Healthcare Holdings (FHH). Thereafter, FHH had announced that it had recruited 50 private medical specialists across Singapore and onboarded Smarter Health, a local healthtech firm, to form the basis of its eventual regional private tech-enabled healthcare ecosystem.

In September 2023, a Singapore-based medical technology start-up company, AWAK Technologies (AWAK), raised US$20 million in Series B funding, one of the largest MedTech fundraise in Southeast Asia in 2023. The funds will be used for AWAK's ongoing human pre-pivotal clinic trial with Singapore General Hospital and enhancing the ultraportable peritoneal dialysis (PD) device in anticipation of a final pivotal trial in the United States commencing in 2025. The wearable PD device allows patients to undergo kidney dialysis at home and on the move.

In November 2023, ObvioHealth, a US- and Singapore-based digital clinical trials provider, had raised S$15 million in its latest funding round.

In December 2023, Doctor Anywhere, a Singapore-based healthcare company, had raised US$40.8 million in a Series C1 extension round. The funds will be directed to drive next-generation healthcare innovation within the company and to deepen its presence in secondary care. The company is poised to enhance its focus on innovating products to establish a vertically integrated digital healthcare ecosystem.

Law stated - 15 January 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

In a legal due diligence exercise, some of the key areas to examine in a digital health venture are as follows:

- Regulatory approvals: all the necessary licences, permits, authorisations and approvals have been obtained by the digital health venture for its business, services or product.
- Intellectual property: the digital heath venture has the necessary intellectual property rights, patents, brands, trademark and/or ownerships for the conduct of its business, services or product.
- Privacy and data protection: ensure that the digital health venture's data protection and privacy policies comply with the provisions of Singapore's Personal Data Protection Act 2012 including adequate data protection policies in place, privacy consents and notices.
- Data security, cybersecurity and information technology (IT): examine the data security measures in place, any IT risks that may lead to operational, financial or commercial exposures.

Law stated - 15 January 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

Venture capital is a common source of financing in the digital health sector in Singapore. In addition, there are increasing non-dilutive government financings in healthcare to meet the rapid demand for medical digital technology innovations.

Notable government financing

The Research, Innovation and Enterprise Plan (RIE2025) was launched by the Singapore government and holds a budget of around S$25 billion, with plans to support new programmes to respond to future needs and emerging opportunities; funds for postgraduate programmes; innovation & enterprise talent development; and to establish new innovation and enterprise platforms to develop entrepreneurial talent. RIE2025 will be organised across four domains, namely: manufacturing, trade and connectivity; human health and potential; urban solutions and sustainability; and smart nation and digital economy.

Other support initiatives

In October 2022, a Clinical Innovation and Adoption Initiative disbursed up to S$1 million to successful applicants to develop and launch their health technologies in hospitals and clinics islandwide.

Healthcare Innomatch is an annual challenge launched in 2021 to gather technology proposals from startups and small and medium enterprises to change the way healthcare is provided in the future. In 2022, S$2.4 million was awarded in funding to six near market-ready solutions. In 2023, three technology startups were the winners of Healthcare InnoMatch 2023 and were awarded a total of up to S$2.4 million to begin test-bedding their innovations.

Law stated - 15 January 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 | What principal legislation governs the digital health sector in your jurisdiction?

While there is no principal legislation that governs the digital health sector in Singapore, there are regulations and guidelines that may be applicable depending on the area of digital health.

The broad scope of digital health includes categories comprising telehealth and telemedicine, mobile health, wearable devices, health information technologies and personalised medicine. Medical devices are defined by the Health Sciences Authority (HSA) as health products that have a physical or mechanical effect when used on human bodies. Some examples of medical devices that incorporate digital health technology are software used by healthcare providers to screen or diagnose, tele-monitoring such as wearable devices, tele-treatment, and digital therapeutics such as software or mobile applications. Medical devices in Singapore are regulated under the Health Products Act and Health Products (Medical Devices) Regulations 2010 and there are regulatory guidance documents issued by the HSA as well for medical devices. Furthermore, the Artificial Intelligence in Healthcare Guidelines was published in October 2021 and serves as a guide for developers and implementers of AI in healthcare and complements the existing HSA regulatory requirements of AI Medical Devices.

Pursuant to the Healthcare Services Act 2020 (HCSA) replacing the repealed Private Hospitals and Medical Clinics Act 1980 on 18 December 2023, telemedicine services are now licensable under the HCSA. Currently, only direct doctor and/or dentist-led teleconsultations are licensable under the HCSA as MOH adopts a risk-based regulatory approach to healthcare services. Other forms of telemedicine (TM) services, such as telecollaboration and telesupport for administrative purposes, will not be licensed under the HCSA.

Law stated - 15 January 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

In Singapore, the healthcare sector in Singapore is generally overseen by the Ministry of Health (MOH). MOH also has a dedicated national health-tech agency, Integrated Health Information Systems (IHiS), that focuses on developing and integrating technology within Singapore's public healthcare sector.

Digital health products (as long as they qualify as medical devices) are principally regulated by the HSA. The HSA administers and enforces the Health Products Act 2007 and its subsidiary legislation, whereas telemedicine services are regulated by the Private Hospitals and Medical Clinics Act 1980 (PHMCA), which will be gradually replaced by the HCSA. The PHMCA and HCSA are administered and enforced by MOH.

There are several regulatory instruments that relate to data protection and privacy in the digital health sector such as the PHMCA and the HCSA, which contain provisions relating to the protection of confidential information such as patients' medical records, diagnosis or treatment, and the Healthcare Cybersecurity Essentials, which provides intermediate and long-term care services in adopting basic safeguards for IT assets and data.

Law stated - 15 January 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

Medical devices in Singapore, including digital health products and services, are regulated under the Health Products Act (HPA), and Health Products (Medical Devices) Regulations 2010, which are governed by the HSA.

In relation to the registration of medical devices, the registration process will differ depending on the device's risk classification and evaluation routes. The risk classification of devices may fall under four classes, Classes A, B, C and D, whereby Class A devices are exempted from product registration. The evaluation route, which determines whether an application for a licence is necessary, depends on three factors: the risk classification, the number of prior approvals by HSA's overseas reference regulatory agencies and the duration of safe marketing history for the device.

As for the licensing requirements, all medical device dealers are required to apply for a dealer's licence (includes importer's, manufacturing and wholesaler's licences) before importing, manufacturing and supplying devices in Singapore, which includes the distribution of digital health products. In granting a dealer's licence, the HSA will also take into consideration whether these dealers have conformed to the requirements of the Good Distribution Practice for Medical Devices, which apply to medical devices incorporating digital solutions (sensors). Information on the software version being registered and to be supplied in Singapore is to be clearly presented on the device labelling (if supplied in

physical form) or software graphical interface (if supplied without physical form), depending on the mode of supply of the software. Further guidelines on licensing requirements specific to software medical devices (such as software embedded in medical devices, standalone mobile applications, standalone software and web-based software) are set out in the Regulatory Guidelines for Software Medical Devices dated April 2022.

Telemedicine providers such as independent doctors/dentists offering teleconsultations themselves or organisations who hire or engage doctors and/or dentists to provide teleconsultations as part of the organisation's services, are required to obtain a licence from the Ministry of Health under the Healthcare Services Act for telemedicine services. Such providers are required to hold an Outpatient Medical Service or Outpatient Dental Service licence with approval for the remote mode of service delivery. However, TM platforms and applications' providers providing software as a service to doctors and dentists will not be licensed under the HCSA.

The covid-19 pandemic has accelerated the use of digital health technologies in clinical trials. The development of electronic consent systems and patient portals has made the enrolment process much smoother, whereby patients are able to access all the information in connection with the clinical trial and provide their consent digitally. HSA would have to be consulted prior to implementation of any digital clinical trial. For instance, an AI-driven digital medicine platform called Quadratic Phenotypic Optimisation Platform (QPOP) was developed by researchers from the Cancer Science Institute of Singapore, which is helping doctors make better clinical decisions when treating cancer patients. QPOP has already proved to be successful in current and past cancer patient trials.

Law stated - 15 January 2024

Soft law and guidance

9 | Is there any notable 'soft' law or guidance governing digital health?

There are notable 'soft' laws and regulations governing digital health. For instance, medical devices in Singapore are regulated under the Health Products Act and Health Products (Medical Devices) Regulations 2010 and there are regulatory guidance documents issued by the HSA. Furthermore, the Artificial Intelligence in Healthcare Guidelines was published in October 2021 and serves as a guide for developers and implementers of AI in healthcare and complements the existing HSA regulatory requirements of AI Medical Devices. Separately, telemedicine services are regulated under the MOH's 2015 National Telemedicine Guidelines, the SMC Ethical Code and the 2016 Handbook on Medical Ethics.

There are further key regulations in Singapore that apply to digital health applications that are considered medical devices:

- Medical Devices Regulations: these regulations deal with the manufacture, import, supply requirements and exemptions for medical devices, presentation, advertisement and registration of medical devices, and various duties and obligations of manufacturers and importers of medical devices.
-

National Telemedicine Guidelines (January 2015): these non-legally binding guidelines were issued by the MOH as a guide setting out best practices in implementing telemedicine solutions. They govern the use of technology and equipment in telemedicine.

- Regulatory Guidelines for Telehealth Products (April 2019): these guidelines describe telehealth products, which may include digital health applications that are categorised as medical devices and set out the risk classification and regulatory controls for telehealth medical devices and standalone mobile applications that are categorised as medical devices.
- A regulatory guidance issued by the HSA in June 2018 that provides guidance on medical device advertisements and sales promotion.
- Guidelines for Telepharmacy 2009 issued by the Pharmaceutical Society of Singapore.

Law stated - 15 January 2024

Liability regimes

10 What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

In Singapore, contractual and tort law would be the key liability regimes applicable to digital health products and services. For example, a contractual claim may arise where there is a breach of contract pertaining the digital health product or service provided. Actions for injuries or damage due to faulty digital health products will be founded on the tort of negligence and breach of contract (if there is privity of contract). Another instance would be actions for breach of patient confidentiality or data breaches which could amount to tort of breach of confidence.

There are also general liability regimes for consumer protection that would be applicable to digital health products and services. For instance, the Consumer Protection (Fair Trading) Act 2003 protects consumers from unfair practices by commercial suppliers (including suppliers of digital health products). In the event of a breach or unfair practices, consumers or customers may obtain civil remedies against these suppliers under contract and tort law and legislations, such as the Unfair Contract Terms Act 1977 and under the Sales of Goods Act 1979 (for example, if the digital health product does not correspond with the description, quality, sample provided or is not fit for purpose).

With regards to cross-border provision of digital health products and services, liability under the law of contract would depend on the laws that the contract is governed by. As regards cross-border tort disputes, this would depend on the country in which the damage occurs or where in substance the tort had occurred. Legal liability issues could arise especially in situations of freelance registered doctors in telemedicine negligence or claims against foreign telemedicine providers. In any event, the common law of the tort of negligence will continue to apply to telemedicine in connection with the diagnosis, advice and treatment by a doctor.

Law stated - 15 January 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

The term 'health data' is not specifically defined under any Singapore legislation. However, the Personal Data Protection Act 2012 (PDPA) in Singapore governs the collection, use, disclosure, retention and care of personal data. The PDPA applies to all industries, including the healthcare industry. As such, 'health data' would be covered under the umbrella term of 'personal data'. Even though the PDPA does not have a special or separate category of 'sensitive' personal data, the Personal Data Protection Commission (PDPC) does take a stricter view when considering a case where the personal data compromised is of a sensitive nature. It is conceivable that the data of a person's health and medical condition, together with other identifying information, can constitute 'sensitive' personal data.

There is no legal definition of anonymised personal data. The PDPA has issued Advisory Guidelines on PDPA for Selected Topics in which the general term 'anonymisation' is referred to as the process of converting personal data into data that cannot identify any particular individual and, depending on the specific process used, can be reversible or irreversible. This would be the best aid to the interpretation as to what constitutes 'anonymised data'.

Law stated - 15 January 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

As 'health data' falls under personal data that is governed under the Personal Data Protection Act 2012 (PDPA), the provisions of the PDPA apply. The PDPC and Ministry of Health have issued Advisory Guidelines for the Healthcare Sector (revised on 28 March 2017), which aim to address the unique circumstances faced by the healthcare sector in complying with the PDPA. There is a greater emphasis in the level of protection afforded to health data in Singapore in view of the importance placed on health data (such as medical records, contact information and financial details) and increases in data breaches, cyberattacks and cybercrime activity. As health data may in some circumstances be considered as 'sensitive' data, the PDPC expects a higher standard of protection for sensitive personal data.

Law stated - 15 January 2024

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

The PDPC and Singapore Digital issued a Guide to Basic Anonymisation on 31 March 2022 that includes references to anonymisation of health data. In relation to healthcare data, the right choice of anonymisation techniques would have to be applied. For instance, the organisation would likely require someone with sufficient healthcare knowledge to assess a record's uniqueness, namely, to what degree that it is identifiable or re-identifiable. Another instance is when data attributes are swapped between records and it takes a healthcare expert to recognise whether the anonymised records make sense. Anonymised health data is also subjected to the Advisory Guidelines for the Healthcare Sector (revised on 28 March 2017).

Law stated - 15 January 2024

Enforcement

14 | How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The data protection laws in Singapore are governed under the PDPA, which includes health data. The PDPC oversees the compliance and enforcement of the PDPA. In relation to health data, the Personal Data Protection Commission and Ministry of Health (MOH) have issued Advisory Guidelines for the Healthcare Sector (revised on 28 March 2017) that aim to address the unique circumstances faced by the healthcare sector in complying with the PDPA.

In June 2018, the nation's worst data breach occurred, with a cyber-attack on SingHealth that resulted in the personal information of 1.5 million patients being compromised. Due to the breach, the technology vendor for Singapore's healthcare sector, Integrated Health Information Systems was fined S$750,000 for lapses in securing patient data and SingHealth, who was the owner of the patient database system, was fined S$250,000 by the PDPC.

In November 2022, Farrer Park Hospital was fined S$58,000 over a data breach that resulted in the medical records of individuals being leaked. The PDPC warned of the risks of such data breach involving sensitive personal data and the need for stronger security arrangements.

Law stated - 15 January 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

To the extent that digital health offerings are closely intertwined with Critical Information Instructure, as defined under the Cybersecurity Act, the provisions of the Cybersecurity Act will apply.

The MOH has issued a guideline on the Healthcare Cybersecurity Essentials (HCSE) in August 2021. The aim of the HCSE is to provide guidance to all healthcare providers on basic cybersecurity measures that can be adopted to ensure the security and integrity of their IT assets, systems, and patient data. While the HCSE is non-binding, healthcare providers are strongly encouraged to adopt the recommended measures. The key recommended measures that healthcare providers can implement are split into three steps: (1) to create an IT assets inventory; (2) to secure the data, detect, respond to, and recover from breaches; and (3) to implement the measures into practices.

The MOH issued the Cybersecurity Advisory 1/2019 in view of the 2018 SingHealth data breach that involved the health data of 1.5 million individuals being leaked. This Advisory set out the cybersecurity best practices arising from the recommendations in the Committee of Inquiry (COI) report to the cyber-attack on SingHealth. In the report, the COI made 16 recommendations to protect SingHealth and other public sector IT systems that contain large databases from cybersecurity attacks.

The MOH and other agencies in Singapore in 2022 began a consultation into the proposed cybersecurity labelling scheme for medical devices (CLS (MD)), which describes a four-tier cybersecurity rating scale. The scope of CLS (MD) would apply to medical devices that handle health-related data or connect to other devices, systems and services.

Law stated - 15 January 2024

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Digital health companies and businesses handling raw and anonymised data should ensure that they comply with the PDPA of Singapore and the relevant guidelines issued by the PDPC such as the Guide to Basic Anonymisation issued on 31 March 2022 and the Advisory Guidelines for the Healthcare Sector revised on 28 March 2017. Digital health companies and businesses should also carefully consider the personal information that they require and the purpose for such information and evaluate the need for transfer or sharing of this personal data.

Digital health companies should ensure there is adequate protection and security of users' raw data and anonymised data, whether stored in-house or with external parties.

In a scenario where data has to be transferred out of Singapore, there is a need to ensure compliance with section 26 of the PDPA (Transfer Limitation Obligations), which limits the ability of an organisation to transfer personal data outside of Singapore.

Law stated - 15 January 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

In relation to digital health-related inventions, the general rules under the Patents Act 1994 would be applicable. Patents are given and protected under the Intellectual Property Office of Singapore. When applying for patents in Singapore, the digital health-related invention must meet certain legal requirements for a patent to be filed. First, the invention must be novel, and this fact may be ascertained by applying a worldwide test of novelty that contains two steps: (1) whether it was anticipated by a previous patent and (2) whether it was published or used anywhere in the world. Second, the invention must involve an inventive step, which means that such inventive step used in creating the invention must not have been obvious to a person skilled in that particular field. Third, the invention must be capable of industrial application, meaning that the invention can be made or used in any kind of industry, including medicine, and serves a useful purpose.

Law stated - 15 January 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

The registration of IP works in a manner that higher priority is accorded to the applicant who files the earliest. This also prevents a similar invention from obtaining the rights and precedence before said applicant.

In May 2022, the Intellectual Property Office of Singapore (IPOS) had launched the SG Patent Fast Track programme (now renamed as SG IP FAST) to support the acceleration of patent applications in all technology fields, including digital health technologies. To begin filing for a patent, the applicant must submit a patent application to the IPOS online and ensure the conditions to qualify or remain on the SG IP FAST programme are met.

While obtaining a patent in Singapore generally takes about two to four years from the date of filling, the accelerated timelines under the SG IP FAST programme grants straightforward patent applications as fast as six months and grants non-straightforward patent applications as fast as nine months. Once granted, the patent takes effect immediately and lasts for 20 years starting from the date that the patent application was filed.

Law stated - 15 January 2024

Other IP rights

19

Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

To the extent a medical device is involved in the service offering, then Registered Design protection may be relevant to protect the shape of the design. A registration for the design would protect the external appearance of the article and have the right to control its use. Similarly, if the digital health offering is performed under a brand, then trademarks to protect this brand may be relevant.

Law stated - 15 January 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

There are only two major practical considerations to take into account when licensing IP rights in digital health technologies:

- whether the licensing terms comply with any regulatory requirements; and
- what is the optimal tax position for the structure of the licence.

Law stated - 15 January 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

The usual court procedures under Singapore Intellectual Property (IP) law generally would be available to IP owners to enforce their rights in digital health technologies.

For any infringement of patents, applicants could bring an infringement action to obtain damages in a civil claim.

In Singapore, the Ministry of Law has announced that in the new Supreme Court of Judicature (Intellectual Property) Rules 2022 that came into force on 1 April 2022, a new optional track for IP litigation will be implemented. The new optional track is streamlined and aims to lessen time costs and for IP dispute resolutions to be more cost-effective. The new track would be mainly for disputes involving an IP right where the monetary relief claimed by each party in the action does not or is likely not to exceed S$500,000 or all parties agree to the application of this simplified process to their case.

There have not been any notable reported cases concerning enforcement actions and digital health technologies in Singapore.

Law stated - 15 January 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

In relation to advertisements for digital health products and services that qualify as medical devices, the Health Sciences Authority has issued a regulatory guidance in June 2018 on medical device advertisements and sales promotion. It is the responsibility of the advertiser to ensure compliance with the legislations and guidelines for advertisement and promotions of medical devices. The advertiser has to take note of the advertisement prohibitions (for instance, advertising to the general public that claim, indicate or suggest that the medical device will prevent, alleviate or cure some diseases or conditions is not allowed) and general principles of advertisements (such as truthfulness, substantiation, accuracy, claims of safety, etc). It is an offence to advertise false or misleading information relating to therapeutic products or medicinal products and these would include digital health products and services.

Law stated - 15 January 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

The general rules governing e-commerce are applicable to digital health offerings. Electronic payments in Singapore are regulated under the Payment Services Act 2019 (PSA). Payment services can only be offered by licensed payment service providers under the PSA, regulated by the Monetary Authority of Singapore. As such, providers of digital healthcare can work with various licensed service providers to provide electronic payments options, increasing accessibility of healthcare to all consumers in Singapore.

In addition, the Health Sciences Authority has set out certain regulatory requirements for licensed retail pharmacies to satisfy if they wish to supply registered therapeutic products, prescription-only medicine and pharmacy only medicines, through e-pharmacy service. An applicant who qualifies to supply registered therapeutic products through the mode of e-pharmacy must implement good governance and practices in operations and operate an effective system to ensure high-quality medicines are supplied to patients. Guidance documents are issued to better understand the specific regulatory requirements to supply registered therapeutic products through e-pharmacy service such as Guidance Notes on Supply of Registered Therapeutic Products through e-pharmacy and Guidance Notes on Good Distribution Practice.

Law stated - 15 January 2024

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Certain digital health products and services are covered or reimbursed by Singapore's healthcare system and private insurers. For example, the Ministry of Health has introduced the Table of Surgical Procedures, which is a patient financing tool that identifies procedures (including robotic-assisted surgery) that qualify for use of MediSave (a national medical savings scheme) funds or claimable under MediShield Life (a basic health insurance plan).

In 2015, the Health Promotion Board (HPB) under Singapore's healthcare system, launched the National Steps Challenge for members of the public where Singapore residents may collect a digital health product, HPB Fitness Tracker, to track the number of steps that they have taken and are rewarded instantly for meeting various milestones stated in the Challenge.

Private insurers have been active in the digital healthcare space and have partnered with various telemedicine services to provide digital healthcare services. For example, under the AIA HealthShield insurance, individuals under the plan would be able to leverage the partnership that AIA has with White Coat (a Singapore-based healthcare provider that offers on-demand telemedicine services through a mobile app) to have a video consultation by Singapore-registered doctors at low costs.

In April 2020, Prudential Singapore launched an artificial intelligence-powered mobile app called Pulse by Prudential that provides Singapore residents with 24/7 access to healthcare services and updates on their health information (for example, being able to check their symptoms, conduct digital health assessments and seek health advice when required).

Law stated - 15 January 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

In July 2023, the Ministry of Health (MOH) launched the Industry Transformation Map (ITM) 2025 for healthcare, which focuses on four main areas:

- strengthening Singapore's research and innovation ecosystem;
- strengthening digital system enablers;
- attracting and retaining healthcare workers; and
- strengthening partnerships.

ITM 2025 also aims to accelerate clinical adoption of research, promote a more efficient use of data and adoption of artificial intelligence (AI).

In July 2023, Singapore's national health technology agency, Integrated Health Information System (IHiS), signed a memorandum of understanding with Microsoft for deeper collaboration in generative AI and cloud innovation. The organisations have collectively agreed to utilise Microsoft Azure and security technology to develop Secure GPT for healthcare professionals. The generative AI application will automate some healthcare tasks for greater efficiency and for healthcare workers to better focus on caring for patients. This collaboration marks an evolution of the way that healthcare is supplied to ameliorate the health of individuals daily in Singapore.

Following this, IHiS was rebranded as 'Synapxe' and aims to deliver more efficient care by applying advanced deep learning and AI capabilities in healthcare. Synapxe now serves as the national health technology agency, actively integrating AI into various projects that focus on addressing critical healthcare challenges including diagnostics (for example: deep-learning AI software system to detect potential threatening eye conditions and predicting the severity of pneumonia in patients), patient admissions and readmissions, and overall management.

As of December 2022, the National Electronic Health Record (a central repository of patient summary health records) was made accessible to all public healthcare institutions and over 30 per cent of private MOH-licensed healthcare institutions, including over 90 per cent of private hospitals, nursing homes and over 60 per cent of medical clinics.

In April 2022, Biofourmis, Singapore's HealthTech startup (and now US-headquartered) surpassed unicorn status with a S$300 million Series D investment. With this investment, Biofourmis intended to scale up its virtual care offerings. This includes delivering personalised and predictive in-home care to a growing number of acutely ill patients and expanding its recently announced virtual specialty care services, Biofourmis Care, to those patients with complex chronic conditions.

Several telemedicine applications have picked up speed in recent years, with digital health applications such as Speedoc and Doctor Anywhere raising funds in various series of funding. Furthermore, Speedoc is MediSave-accredited and Community Health Assist Scheme-accredited (CHAS-accredited), which makes the application more attractive to Singapore residents as they will be able to use CHAS subsidies and MediSave to subsidise part of their healthcare bills.

Law stated - 15 January 2024

RHTLaw Asia

Erwan Barre erwan.barre@rhtlawasia.com
Wun Rizwi rizwi.wun@rhtlawasia.com

RHTLaw Asia LLP

South Korea

Tae Uk Kang, **Juho Yoon**, **Hyo-Jun An**, **Susan Park**, **Ahwon Choi**
Bae, Kim & Lee LLC

Summary

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

Key players active in South Korea's digital health market largely consist of conglomerates, healthcare companies, large hospitals and government-affiliated organisations. The digital health sector in South Korea has traditionally been subject to considerable legal regulations and restrictions and only recently has the South Korean government started to ease regulations in light of the need to develop 'untact' industries. A prime example of such measures is the use of pseudonymised information in healthcare. In August 2020, provisions regarding pseudonymised information were newly added to the Personal Information Protection Act (PIPA), the main legislation governing the protection of personal information in South Korea, opening up the possibility of using pseudonymised information in healthcare. Subsequently, in September 2020, the relevant regulatory authorities co-published the Guidelines for Use of Health-Medical Data to further specify the permitted practices in connection to pseudonymisation methods and procedures. This was amended in January 2021 and further amended in December 2022, after gathering opinions from industry stakeholders. In addition, the South Korean government has expressed its intention to utilise pseudonymised information in sharing government-owned big data relating to health insurance to support the development of new drugs and medical technologies. Relevant government authorities and organisations, such as the Ministry of Health and Welfare and the Korea Health Industry Development Institute, have been consistently organising and hosting related forums, seminars and academic conferences on this subject matter. Further, in 2022 alone, a couple of new bills have been introduced into the National Assembly: one, in support of the promotion of digital healthcare and utilisation of health-medical data, and another for the promotion and support of digital healthcare businesses. In addition, in September 2023, a similar bill (Act on Digital Healthcare and Healthcare Data Utilization) was proposed to the National Assembly, which aims to define and promote the utilisation of digital healthcare and health-medical data.

Law stated - 30 January 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

Regulations regarding digital health technologies and the related use of personal information are still considerably stricter in South Korea compared to other countries. For example, even though provisions regarding pseudonymised information were newly added to PIPA in 2020, such provisions still limit the use to strict standards. In addition, telemedicine between healthcare professionals and patients is still prohibited under the Medical Service Act. Accordingly, although there is ample investment interest in the sector, the investment climate is inevitably impacted by strict regulations.

Law stated - 30 January 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

In February 2020, GC Healthcare (a subsidiary of GC Pharma, which is a major South Korean pharmaceutical company), acquired UBcare Co Ltd, the largest electronic medical record company in South Korea, for 208.8 billion South Korean won. In addition, Lunit Inc, a medical diagnosis artificial intelligence (AI) deep learning startup, was included in CB Insights' Digital Health 150 for 2019 and 2020 consecutively, which attracted investment from a number of venture capitals and financial investors, both local and abroad. Last, in August 2021, it was reported in the media that Naver Corp, South Korea's leading search engine service provider, is in talks to acquire a 10 per cent stake in ezCaretech Co, Ltd, a South Korean cloud electronic medical records company. If this deal is finalised, Naver's acquisition will likely have a significant impact on the South Korean digital healthcare industry, as ezCaretech currently enjoys a 50 per cent market share in the market based on the top 10 hospitals in South Korea.

Law stated - 30 January 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

Since there are considerable regulations related to healthcare in South Korea, it would be necessary for investors to carefully review and consider whether the particular company or service would be legally feasible in South Korea: the relevant regulations, position of the competent regulatory authorities and so on.

Law stated - 30 January 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

Venture capitalists and financial investors are actively investing in equity, and in some cases, they are directly acquiring companies. In July 2020, the South Korean government finalised and announced the Korean New Deal Comprehensive Plan. According to this plan, the South Korean government plans to invest 160 trillion South Korean won in digital new deal (data, 5G, AI, information and communications technology-based business across

all industries, digital health, etc), green new deal (ecosystem recovery) and social safety net reinforcement (resolving economic inequality) by 2025, creating 1.9 million jobs in the process.

Law stated - 30 January 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 What principal legislation governs the digital health sector in your jurisdiction?

There is no single piece of legislation governing the digital health sector. As such, the current key legislation would be both the Personal Information Protection Act (PIPA) and the Medical Service Act (MSA). In addition, with regard to health data, the following legislation applies:

- the Pharmaceutical Affairs Act;
- the Medical Devices Act;
- the Bioethics and Safety Act; and
- the National Health Insurance Act, etc.

However, similar terms or concepts are defined slightly differently under each piece of legislation, and each includes provisions that may require separate consent procedures for the use of personal information or otherwise limit such use. There is indeed a need to reorganise legal regulations related to the digital health sector. The aforementioned newly proposed bills are intended to streamline and distinguish the multi-level interplay of the different laws.

Law stated - 30 January 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

Regarding personal information, the Personal Information Protection Committee (PIPC) became the primary regulatory body as a result of the major amendments to PIPA, which took effect in August 2020. Further, other regulatory bodies may have jurisdiction over certain matters depending on which law applies, such as the Ministry of Health and Welfare (MOHW) (eg, the MSA, the Bioethics and Safety Act and the Framework Act on Health and Medical Services) and the Ministry of Food and Drug Safety (eg, the Medical Device Act and the Pharmaceutical Affairs Act).

Law stated - 30 January 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

The provision of digital health services is generally regulated by the MSA, but there are two noteworthy limitations: first, the MSA currently only allows the provision of medical services by healthcare professionals (namely, doctors, dentists, oriental doctors, midwives and nurses, all licensed by the MOHW). Consequently, certain digital health services that may be classified as 'medical services' under the MSA cannot be provided by non-healthcare professionals. Regarding the scope of medical services under the MSA, the Supreme Court has construed this to mean:

> prevention or treatment of diseases by performing examinations, optometry, prescriptions, medications, or surgical procedures, with experience and skills based on medical expertise, and other acts that may cause harm to health and hygiene if not performed by a healthcare professional.

Further, in the Guidelines for Non-Medical Health Management Services (first) published by the MOHW in May 2019, the scope of 'medical services' is detailed as:

> acts such as examination, diagnosis, prescription, treatment, procedure, surgery, guidance, etc, that are performed based on medical expertise and skills.

Second, the MSA currently only allows telemedicine between healthcare professionals, and telemedicine between healthcare professionals and patients is prohibited. However, the South Korean government has been operating a regulatory sandbox for the past couple of years and starting with a wristwatch-type electrocardiogram in 2019, the government has permitted more than 55 cases of telemedicine-like services (eg, an arrhythmia telemetry monitoring service, a patient health information monitoring device service, an elderly health-risk detection service and an online treatment and consultation service for South Koreans overseas), possibly moving towards the introduction of telemedicine between healthcare professionals and patients. In addition, the MOHW is permitting in-person treatment of covid-19 patients temporarily. Further, if digital healthcare products qualify as medical devices under the Medical Device Act, reports or registrations in connection to manufacturing, import, sales and rentals must be filed with the Ministry of Drug and Safety (MFDS) for the purposes of verifying safety, efficacy, etc. In accordance with the Pharmaceutical Affairs Act, any clinical trials must also be conducted after obtaining approvals from the MFDS. Last, for medical devices to be incorporated into the national health insurance fee system, time-consuming procedures such as medical technology evaluations and insurance registration procedures must be completed.

Law stated - 30 January 2024

Soft law and guidance

9 | Is there any notable 'soft' law or guidance governing digital health?

The regulatory bodies in South Korea have published numerous 'soft' guidelines relating to digital health. For example, the MOHW published the Guidelines for Non-Medical Health Management Services (first) (May 2019), the PIPC published the Guidelines on Processing Pseudonymised Data (September 2020, as further amended in October 2021 and April 2022), and the MOHW and the PIPC also co-published the Guidelines for Use of Health-Medical Data (September 2020, as further amended in January 2021 and December 2022). The guidelines are provided by the relevant regulatory body to help industry stakeholders better understand the law and technically are not legally binding. However, because these guidelines reflect the regulatory body's interpretation and position regarding the law, it is recommended that these guidelines be taken into consideration and observed as much as practicable.

Law stated - 30 January 2024

Liability regimes

10 | What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

In South Korea, the key liability regime applicable to digital health products and services would be an administrative liability. This is because the provision of products and services of this nature is mainly regulated by government bodies in accordance with relevant laws, and administrative sanctions are imposed in the case of violations. In addition, product liability, tort liability, criminal liability, consumer protection liability and contractual liability vis-à-vis consumers are all generally applicable to digital health products and services provided to the public. There are no particular exceptions to the cross-border provision of digital health products and services.

Law stated - 30 January 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 | What constitutes 'health data'? Is there a definition of 'anonymised' health data?

No law specifically defines 'health data' per se, but 'health information' is categorised as a type of sensitive information under article 23 of the Personal Information Protection Act (PIPA). According to the Guidelines for Use of Health-Medical Data co-published by the Ministry of Health and Welfare (MOHW) and PIPA in September 2020, 'health information' includes but is not limited to the following:

- medical records and electronic medical records under the Medical Service Act (MSA), and other records produced in hospitals that indicate or easily enable the indication of medical treatment details (eg, hospital receipts containing medical treatment details);
- data for insurance claims collected by the National Health Insurance Service, the Health Insurance Review and Assessment Service, and other private insurance companies, data related to health, illness, injury, etc, used in the subscription design and ancillary data;
- health examination data, health examination result data;
- health status information diagnosed by a physician, measured by medical devices, or identified or estimated through estimation of insurance claim records, other algorithms, etc; and
- information collected through medical devices to measure health status or health habits (eg, number of steps, heart rate, oxygen saturation, blood sugar, blood pressure and electrocardiogram).

In particular, if information that is normally not considered health information is used for the diagnosis, treatment, prevention or management of diseases, such information will also be viewed as health information (eg, a voice recording is not health information under normal circumstances, but if the risk of disease is predicted using a voice recording, that voice recording file will be considered health information). Meanwhile, pseudonymised information refers to personal information that has been processed, such as deletion or replacement of certain parts, so that a specific individual cannot be identified without additional information (article 2 of PIPA), and anonymised information refers to personal information that can no longer be used to identify a specific individual even if additional information is used in reasonable consideration of time, cost and technology (article 58-2 of PIPA). Anonymous information is not subject to PIPA. In addition, the Bioethics and Safety Act defines 'anonymisation' as the permanent deletion of personally identifiable information or full or partial substitution of personally identifiable information with an identification code assigned by an institution (article 2). Therefore, anonymisation under the Bioethics and Safety Act is construed as being conceptually similar to pseudonymisation under PIPA. Because there exist discrepancies in definitions between different laws, it is necessary to carefully review and determine the applicable law on a case-by-case basis when actually processing health data.

Law stated - 30 January 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Personal information protection in South Korea is principally governed by PIPA. PIPA is similar to the EU General Data Protection Regulation in terms of structure and principle, but consent is regarded as the main lawful basis for the use and processing of personal information under PIPA. In particular, health data (or health information) is

categorised as a type of sensitive information under article 23 of PIPA. Sensitive information must be obtained through separate consent from the data subject, apart from other general personal information, and PIPA provides for stronger legal protection to sensitive information compared to regular personal information (eg, security measures to prevent the loss, theft, leakage, forgery, alteration or damage of sensitive information are required). In addition, in the case of medical records, the MSA specifically defines and regulates matters related to its recording, access, provision to third parties, electronic medical records, etc. Violation of such provisions of PIPA and the MSA may result in administrative sanctions and even imprisonment.

Law stated - 30 January 2024

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

As a bottom line, personal information is subject to PIPA and its subordinate legislation. In particular, in light of the newly added provisions to PIPA in 2020, personal information controllers may process pseudonymised information without the consent of data subjects for the purposes of statistics, scientific research and archiving in the public interest. Such pseudonymised information may then also be provided to third parties without the consent of data subjects, as long as such provision is within the scope of the above purposes. However, to process pseudonymised information, various measures to ensure stability (managerial, technical and physical) specified in the Presidential Decree must be in place, regarding which the Personal Information Protection Committee (PIPC) published the Guidelines on Processing Pseudonymised Data to serve as general guidance. Meanwhile, specifically regarding pseudonymised health information, the MOHW and the PIPC also co-published the Guidelines for Use of Health-Medical Information in September 2020 (further amended in January 2021 and December 2022). In addition, while there is no clear guideline specifically regarding anonymised information under PIPA, the aforementioned two sets of guidelines also include explanations on anonymised information, and therefore, they should be referred to as applicable. However, because anonymisation under the Bioethics and Safety Act is conceptually similar to pseudonymisation under PIPA, when anonymising personal information under the Bioethics and Safety Act, the aforementioned two sets of guidelines will directly apply.

Law stated - 30 January 2024

Enforcement

14 | How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

In general, regulations on personal information, including health data, are relatively strict in South Korea. In particular, the PIPC, which became the new primary regulatory body as a result of the major amendments to PIPA in 2020, has expressed on many recent occasions

its intention to regulate issues relating to personal information protection considerably more rigorously than before, regardless of domestic or offshore businesses. Meanwhile, when it comes to any notable regulatory or private enforcement actions with regard to digital healthcare technologies in particular, during the period 2011–2015, the Korean Pharmaceutical Information Center (affiliated with the Korean Pharmaceutical Association) encrypted billions of cases of personal information of patients and physicians (including a large amount of sensitive information, such as name, resident registration number, licence number and dispensing details) registered through its preparation management and evaluation request computer program PM2000 and sold such information to IMS Health Korea, a global medical data company. There were allegations of personal information leakage owing to the low level of encryption, and the affected data subjects brought both civil and criminal claims to court, but the civil court determined that there was no damage caused by the personal information leakage and dismissed the data subjects' claims for damages compensation (currently appealed to the Supreme Court), while the criminal court did not find the defendants guilty on the grounds that it was difficult to determine the wilfulness of the defendants and that the act in question was initiated before 30 September 2011, the date on which PIPA took effect (currently on appeal before the Supreme Court).

Another noteworthy case is SK Telecom's SKT Smart Health Electronic Prescription Service, which launched in October 2011. SK Telecom's service involved electronic prescription information (including sensitive information such as prescription details) prescribed by physicians via an electronic chart computer program, which was then transmitted to and stored on SK Telecom's relay server without consent from the patient, and ultimately transmitted to a member pharmacy upon request at a fixed fee. The service was also alleged to be in violation of PIPA and the MSA, but in September 2020, the Seoul High Court dismissed the allegations based on the grounds that the transmission of personal information could be viewed as a simple relay rather than actual processing of personal information, that encrypted electronic prescription information does not qualify as sensitive information under PIPA, and processors entrusted with personal information from a controller do not have to separately obtain consent from data subjects (currently on appeal before the Supreme Court).

Law stated - 30 January 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

As in other countries, regulations regarding security in South Korea can be categorised into data security regulations and cybersecurity regulations. With regard to data security, PIPA prescribes a list of technical, managerial and physical safety measures to be taken by personal information controllers. This list includes:

- establishing, implementing and inspecting an internal management plan for the safe processing of personal information;
- establishing and implementing measures to limit access to personal information ;
- establishing and implementing measures to control access to personal information;

- measures to ensure that personal information is safely stored and transmitted;
- establishing and implementing measures to store log-in records and prevent forgery or falsification thereof in order to respond to data breaches;
- installation and periodic updates and inspections of a program equipped with functions to ensure that the personal information processing system and personal information handlers can always check and treat any penetration of malicious computer programs such as computer viruses, spyware and ransomware into information devices used for personal information processing; and
- establishing and implementing physical measures for safekeeping of personal information, such as making available storage facilities or installation of security devices (article 30 of the Presidential Decree of PIPA).

Further, to ensure the performance of a personal information controller's obligation for damages to any data subject in the event of a violation of the personal information controller's obligations under PIPA, PIPA requires the personal information controller to take necessary measures, such as signing up for insurance or setting aside reserves (article 39-9 of PIPA). The Presidential Decree of PIPA further details thresholds for which such an obligation applies, but the minimum coverage or reserve amount differs based on sales and the average daily users of the service in the previous year (minimum 50 million South Korean won, maximum 1 billion South Korean won). Meanwhile, under the MSA, healthcare professionals and founders of medical institutions are required to have in place facilities and equipment necessary for managing and storing electronic medical records (EMR) safely, and when an addition or revision is made to EMR, such access records shall be separately stored (article 23 of the MSA). Details of these requirements are provided in article 16 of the Presidential Decree of the MSA, as well as the Standards on Facilities and Equipment Required for Management and Preservation of Electronic Medical Records published by the MOHW. To give a few examples, the Standards explain details on backup storage equipment for the EMR, facilities and equipment related to network and system security, facilities and equipment to prevent physical access to EMR storage locations, facilities and equipment for real-time inspection of EMR systems, spare equipment, surveillance equipment such as closed-circuit television and disaster-prevention facilities.

With regard to cybersecurity, the Act on the Promotion of Information and Communications Network Utilisation and Information Protection requires IT service providers (data controllers) and, if applicable, their data processors to take technical, managerial and physical measures to ensure the safety of the security of the information and communications network and the reliability of the information. Such measures include, inter alia, requirements to:

- establish and operate an internal information protection organisation;
- establish and implement an internal personal information management policy;
- ensure personnel security;
- prevent unauthorised access to personal information by controlling access authority and implementing technical measures to control access;
- encrypt important information; and
- retain logs for a certain period of time.

Law stated - 30 January 2024

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

As the law and relevant guidelines already stipulate in detail matters such as the retention, use and provision of personal information and also pseudonymised information, the best practice would be to consider and observe the same as much as practicable. However, there are a number of uncertain or unprecedented issues, as South Korea is only now in the early stages of deregulation of the digital healthcare sector. Still, the South Korean government has indicated that it is aware of the necessity of fostering and developing the digital healthcare sector, and there is a visible trend toward easing existing regulations.

Law stated - 30 January 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Digital health-related inventions are generally classified as inventions that require the computer or software to implement. In the patent filing process for such computer-related inventions, the separate evaluation criteria for computer-related inventions apply. Therefore, when filing for patents in connection to digital health-related inventions in South Korea, it is necessary to comply with the specific requirements detailed in the aforementioned evaluation criteria for computer-related inventions. In particular, in the case of patent filing of software, the application must include as claims the use of hardware and mediums and the association between those and the software. In addition, in the case of software patents, the scope of the patent generally tends to be narrowly recognised compared to other patents in practice.

Meanwhile, the Invention Promotion Act applies to digital health-related inventions invented by employees. The Invention Promotion Act defines 'employee's invention' as an:

> invention that an employee, executive officer of a corporation, or public official makes in connection with his or her duties, where it falls within the scope of business of the employer, the corporation, the state, or the competent local government, and the activities that have led to the invention fall within the present or past duties of the employee.

If a digital health-related invention is also an employee's invention, in principle, the right to file an application, etc, lies with the employee who is the inventor, and for the company to obtain this right, the right must be inherited through contract or work regulations. An employee who transfers his or her right to file an application to the company is entitled to receive just compensation from the company. In relation to such payments to employees, the company must prepare compensation rules and inform its employees of the details in writing, and when actually paying compensation according to such compensation rules, the company must inform the recipient employees of specific details, including the compensation amount.

Law stated - 30 January 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

The patent application process for digital health technologies is similar to the general patent application process. In South Korea, patents are applied to and registered with the Korean Intellectual Property Office (KIPO). The patent application and registration process largely comprise the:

- application;
- request for evaluation;
- application disclosure;
- notification of opinion submission; and
- registration of the patent.

When an applicant prepares a specification and applies for a patent to the KIPO, the KIPO, upon evaluation, will notify the applicant of any grounds for registration rejection and accept opinions regarding the same, as well as allow the applicant to submit amendments. If there are no longer any grounds for registration rejection, the KIPO will decide on the registration of the patent and, upon payment of the registration fees, the patent will be officially registered in the Patent Register. Usually, the entire process takes approximately one-and-a-half to two years from application to registration.

Meanwhile, there are many cases in which before filing an application for a patent, prior assessments are conducted to confirm whether patent registration would be impossible owing to the existence of prior patents, etc.

Law stated - 30 January 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Software written in relation to digital health technologies is considered 'computer program work' under the Copyright Act, and thus is protected under the Copyright Act.

In addition, databases accumulated in connection with digital health offerings are also protected similarly to works under the Copyright Act. Under the Copyright Act, a database is defined as 'a compilation whose materials are systematically arranged or composed, so that they may be individually accessed or retrieved'. A creator of a database has the right to reproduce, distribute, broadcast or transmit the database and is also provided remedies under the Copyright Act against those who infringe such rights. Rights to a database last for five years from the completion of production, but if the database is updated, the protection period commences again from the time of the update.

Further, if the software, hardware, database, etc, related to digital health offerings are not publicly known and have an independent economic value and are managed confidentially by the provider, it may qualify and be protected as a trade secret under the Unfair Competition Prevention and Trade Secret Protection Act (UCPTA). If the trade secret is infringed upon, the owner of the trade secret is entitled to file for the prohibition of infringement, claim damages, etc, and may also claim criminal liability.

The UCPTA protects data that is technical or business information provided to a specific person for business purposes and accumulated and managed electronically, even if such information does not constitute a database under the Copyright Act or is not maintained as a trade secret. Specifically, under the UCPTA, the following acts involving data are prohibited:

- acquisition, use, or disclosure of data by fraudulent means by a person without access authority thereto;
- using, disclosing, or providing data to a third party by a person with access rights for the purpose of obtaining unjust enrichment or causing damage to the data holder;
- acquiring, using, or disclosing such data even with the knowledge of the above circumstances; or
- without legitimate authority, providing technologies, services, devices, etc, for the purpose of neutralising technical protection measures applied for data protection.

Law stated - 30 January 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

In practice, when licensing digital health technologies, the subject and scope of the licence may be unclear. If the subject and scope of the licence are unclear, in the event of a dispute, there may be a risk of the licence being deemed to cover certain parts of the technology that were not intended to be included in the licence scope. Therefore, it is advisable to clearly define the subject and scope of the digital health technologies licensed at the time of contract execution.

In addition, in the process of granting a licence, certain matters should be considered and determined appropriately depending on the circumstances: in what format will the licence be granted (exclusivity, customising, etc), how the licence fee will be calculated (eg, in the case of hardware, will it be based on the total number of pieces of hardware sold, the total number of medical devices sold or the number of times the hardware was used, etc?) and so on.

Meanwhile, in the case of licensing IP rights for digital health technologies, if the IP rights transferred to the licensee (assuming the IP rights are recognised under the relevant law) contain personal information about patients or health data, there may be personal information protection issues under the Personal Information Protection Act. Therefore, consent from data subjects must be obtained prior to the execution of the licence agreement or, in the absence of such consent, personal information must be excluded from the scope of the licensing.

Regarding digital health technology, a licensee may invent improved technology in the course of commercialising or further researching the licensed technology. In this case, it is necessary to stipulate in the licence agreement in advance the related matters, such as the attribution of rights and licence of the improved invention, payment of consideration, and the obligations or rights relating to such improved invention after the termination of the licence.

Law stated - 30 January 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

Regarding the enforcement of intellectual property rights, IP rights in digital health technologies do not appear to be particularly different compared to IP rights in other sectors.

Law stated - 30 January 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

If a digital health product qualifies as a medical device (eg, a product used for the purpose of diagnosing, treating, reducing or preventing diseases, etc), it is subject to advertising regulations under the Medical Devices Act. That is:

- false or exaggerated advertisements about the name, performance or efficacy of a medical device;

- advertisements in which a physician recommends or guarantees a medical device; and
- advertisements regarding the name, manufacturing method, performance, efficacy and effect of medical devices that are not licensed or certified, or that are different from those reported, are all prohibited, inter alia (article 24(2) of the Medical Devices Act).

If a digital health product is not a medical device, the usual Act on Fair Labelling and Advertising applies. Similar to the Medical Devices Act, the Act on Fair Labelling and Advertising prohibits:

- false or exaggerated labelling or advertising;
- deceptive labelling or advertising;
- unfairly comparative labelling or advertising; and
- slanderous labelling or advertising (article 3(1) of the Act on Fair Labelling and Advertising).

Law stated - 30 January 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

With regard to digital health offerings to customers, all laws related to consumer protection (eg, the Act on the Regulation of Terms and Conditions, the Act on Door-to-Door Sales, etc) apply. In particular, all transactions conducted in an electronic manner are subject to the Act on the Consumer Protection in Electronic Commerce, Etc. The foregoing Act stipulates the obligations of businesses and the rights of consumers that apply to contracts executed between a business and consumer through the internet. For example, consumers are given the legal right to cancel a contract for any reason within seven days of execution (with certain exceptions) (article 17). Further, when telecommunications services are provided, the Telecommunications Business Act applies, which prohibits acts of telecommunications business operators that harm or may harm fair competition or the interests of consumers.

Law stated - 30 January 2024

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

If a digital healthcare product qualifies as a medical device under the Medical Device Act and has received approval as a medical device, and the service using the digital healthcare product has received a 'new medical technology evaluation', the digital healthcare product and service may be reimbursed by the national healthcare system.

Further, in the case of robots, three-dimensional printing, implantable devices, virtual reality and augmented reality, nanotechnology, artificial intelligence, digital therapy, precision medicine and advanced regenerative medicine, technology in these areas is subject to an 'innovative medical technology evaluation'. The innovative medical technology evaluation was introduced on 15 March 2019 and is a fast-track evaluation system where, when safety is deemed secure for advanced medical technology for which research results are difficult to accumulate, the potential value of such technology, such as dramatically improving patients' lives or reducing patients' cost burden, is additionally evaluated, and the opportunity to enter the market first and receive a post-market re-evaluation is given. In the case of private insurance, it is possible to cover or reimburse the use of medical devices that are digital health products, in accordance with the individual insurance contracts.

Law stated - 30 January 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

The concept of pseudonymised information was introduced for the first time in the Personal Information Protection Act with new provisions added in 2020, making it possible to pseudonymise personal information and process that pseudonymised information. Accordingly, in September 2020, the Ministry of Health and Welfare (MOHW) and Personal Information Protection Committee also co-published the Guidelines for Use of Health-Medical Data (the Guidelines), which was further amended in January 2021 and December 2022, after gathering opinions from the industry stakeholders. With the revision, there has been positive feedback from industry stakeholders, in that previously ambiguous or impractical parts of the Guidelines have been clarified or modified. For example, under the previous Guidelines, any entity seeking to use pseudonymised information was required to establish an internal data review committee. However, the relevant parts of the Guidelines were amended so that entities, including small-sized hospitals, clinics, startups, etc, can now take advantage of a pool of experts provided by the Korea Health Information Service, an agency designated by the MOHW, in forming their respective internal data review committees. Additionally, entities are now allowed to outsource internal data review work if necessary or preferable. Another example of improvement to the Guidelines is the new addition of standard forms of contracts for the provision and use of pseudonymised information in the health and medical fields. Entities are free to utilise these standard contracts as necessary. The Guidelines, as last amended in December 2022, clearly define the standards for pseudonymisation of medical image data, reflecting the opinions of the industry stakeholders. Also, the Guidelines improved the operating standards of an internal data review committee by relaxing the composition requirements. Previously, the committee

consisted of five to 15 commissioners and a majority thereof needed to be from outside MOHW. As amended, the committee is to consist of at least five commissioners and at least two commissioners need to be from outside MOHW (including one person with experience and expertise in personal information protection work, and one person capable of advocating for the data subjects or representing their perspective).

Further, on 30 September 2021, an amendment bill to the Medical Service Act permitting telemedicine was proposed in the National Assembly. The bill allowing telemedicine, which is currently prohibited under South Korean law, would permit telemedicine for clinic-level observation and consultation for patients with chronic diseases such as hypertension, diabetes and arrhythmia. The bill also provided for other related matters, such as liabilities in the case of telemedicine accidents or malpractice. In addition, in 2022 and 2023, a couple of new bills have been introduced into the National Assembly, in support of the promotion of digital healthcare and utilisation of health-medical data, and for the promotion and support of digital healthcare businesses.

All of these recent developments have led to a degree of anticipation regarding the use of medical big data in South Korea.

Law stated - 30 January 2024

Tae Uk Kang taeuk.kang@bkl.co.kr
Juho Yoon juho.yoon@bkl.co.kr
Hyo-Jun An hyojun.an@bkl.co.kr
Susan Park susan.park@bkl.co.kr
Ahwon Choi ahwon.choi@bkl.co.kr

Bae, Kim & Lee LLC

Switzerland

Anne-Catherine Cardinaux
Walder Wyss Ltd

Summary

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

In Switzerland's local digital health market, key players encompass various entities contributing to innovation and development. These players include:

- Academic institutions: eg, the Swiss Federal Institute in Lausanne (EPFL) and the Federal Institute of technology in Zurich (ETH Zurich) are prominent in driving innovation. They foster a conducive environment for research and development, aiding in the emergence of startups through technology transfer initiatives.
- Startup incubators: Institutions such as the EPFL Innovation Park in Lausanne or the Bio-Technopark in Schlieren provide essential support and resources to digital health startups, facilitating their growth and development, and help connect startups with investors and other key players within the venture ecosystem.
- Government-driven programmes: Initiatives such as InnoSuisse play a vital role in providing support to companies in the digital health sector, particularly in their early stages.
- Investors: Switzerland boasts an active investor scene comprising traditional venture capital (pre-seed, seed and post-seed stage, mostly by 'angels', family offices, traditional venture capital funds and the like), private equity funds and large industrial companies. These investors provide crucial financial backing, fostering innovation and growth in the digital health market. Corporate venture investors contribute by sharing knowhow and granting access to industrial networks as well.
- Regulatory agencies: Regulatory agencies such as Swissmedic play a crucial role in ensuring the safety and efficacy of digital health products and services in Switzerland.

Prominent areas of innovation in the Swiss digital health market include telemedicine and remote patient monitoring, healthcare data analytics and artificial intelligence (AI), digital therapeutic and wearable health technologies.

Law stated - 1 March 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

The investment climate for digital health technologies in Switzerland is generally positive, supported by various factors that attract investors. These factors include a strong innovation ecosystem, government initiatives supporting digital health startups and research projects, and access to a diverse range of funding sourcing in a stable economy. Switzerland's

healthcare system is known for its high quality and efficiency, making it attractive for investments in companies focusing on digital health technologies. Moreover, its central location in Europe and its proximity to major healthcare markets such as Germany and France make it an ideal launchpad for companies targeting the broader European market.

However, despite the favourable investment climate, there are also a few challenges in the Swiss digital health sector: Navigating the regulatory landscape can be complex and time-consuming, particularly for startups and early-stage companies. Labour in Switzerland is expensive and compliance with data protection regulations can also present challenges for companies developing digital health technologies (even if less stringent compared to EU regulations).

Law stated - 1 March 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

According to a PwC analysis, the Swiss market experienced a turnaround from the declining trend in health industries. Both the number of deals and their total value in 2023 surpassed those of the previous year. The Swiss life science deal activity is close to historical highs. The notable recent deals in the digital health sector include:

- In Q4 of 2022, Swiss-based medical technology company MedAlliance announced having entered into an agreement with Cordis, a global developer and manufacturer of interventional cardiovascular technologies, for an acquisition.
- In Q1 of 2022, Sonova Holding AG, a Swiss-based leading provider of hearing care solutions, has successfully completed the acquisition of Alpaca Audiology LLC, a large independent networks of audiological care clinics in the US.
- In Q3 of 2021, SOPHiA Genetics, a Swiss-based creator of a global data pooling and knowledge sharing platform, announced the closing of a US$234 million initial public offering and US$20 million private placement.

Law stated - 1 March 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

Before acquiring a stake in digital health ventures, investors should conduct due diligence on several key areas, industry-related and general:

- Regulatory compliance (ensuring adherence to healthcare and data protection regulations).
-

Intellectual property portfolio (assessing the company's patents, trademarks, trade secrets and other IP-related topics).

- Clinical validation and efficacy (evaluating scientific evidence supporting the effectiveness of the product) and the existence of relevant approvals and/or permits for commercialisation.
- Market demand and competition (assessing demand, target demographics and competitive landscape).
- Technology infrastructure and security (reviewing data security measures and technology protocols).
- Business model and revenue generation (understanding how the company plans to generate revenues and reach profitability).
- Team expertise and experience (evaluating the leadership team's track record in the industry).
- Financial viability and projections (reviewing financial statements, business plan, fundraising history and future cash flow planning).
- Customer adoption and retention (examining adoption rates, satisfaction levels and churn rates)
- Partnerships and collaborations (assessing existing and potential partnerships for growth).
- General legal due diligence topics (including assessment of company and share structure, ownership over shares and assets, validity of material agreements, compliance with laws and regulations, insurance coverage, tax, labour, pension and disputes or litigation).

Law stated - 1 March 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

While digital health ventures commonly employ financing structures similar to those used across various sectors, given the typical absence of robust valuation data for early-stage digital health companies, debt securities (instead of shares), typically in the form of convertible notes, are used first to avoid any under-pricing. Such convertible notes convert into shares as part of a future qualified equity financing round, typically at a certain discount to the cash price to be paid by equity investors (said discount in this industry usually being between 10 and 30 per cent, occasionally in addition to any interest payments, typically being between 2 and 10 per cent). Importantly, such debt is 'subordinated' under Swiss law and thus cannot be repaid in cash if the company has no distributable equity. As the company progresses and attains a solid valuation, traditional equity financing rounds become prevalent. For such rounds, customary features are used for digital health venture companies, such as preferred shares (the financial preference often being a 1 x *non-*

-participating liquidation preference, unless in financial distress where investors usually ask for more aggressive terms), board seat, anti-dilution protection (Swiss venture standard being weighted average and not full ratchet!), drag-along and similar rights.

While not specifically targeted at the digital health sector, Swiss federal and cantonal authorities have implemented initiatives to bolster innovation and support early-stage companies. Notable among these is InnoSuisse, the Swiss Innovation Agency. An example on a cantonal level is the Zurich University Hospital's (USZ) Health Innovation Hub. Although these initiatives aren't exclusive to digital health, they aim to foster innovation and R&D, thereby indirectly benefiting ventures in the digital health space.

Law stated - 1 March 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 | What principal legislation governs the digital health sector in your jurisdiction?

Swiss legislation concerning digital healthcare or digital medicine lacks comprehensive coverage. Instead, health-related information technologies are typically categorised within each regulatory framework according to the objectives of the respective regulations.

Swiss laws maintain a 'technologically neutral' stance, seldom addressing specific technologies directly. Depending on their functionalities, attributes and assertions, digital healthcare and digital medicine may fall under various regulatory considerations, including:

- obligations regarding data protection and professional confidentiality (Federal Act on Data Protection (FADP); Data Protection Ordinance (DPO); Swiss Criminal Code; cantonal laws);
- Human Research Act (HRA);
- regulations pertaining to medical devices (Therapeutic Products Act (TPA); Medical Devices Ordinance (MedDO); Ordinance on In Vitro Diagnostic Medical Devices (IvDO);
- professional practice and licensing requirements;
- liability regulations (product liability);
- restrictions on advertising;
- rules regarding the provision of benefits to healthcare professionals (HCPs), healthcare organisations (HCOs), or patient organisations;
- telecommunications regulations; and
- public procurement provisions.

Law stated - 1 March 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

Switzerland operates as a federal state comprising 26 cantons, with one central federal government. The federal government holds responsibility for various sectors including health insurance, medications, medical devices and public health. Conversely, the cantons oversee hospital planning, licensing of service providers, and possess significant autonomy in organising their respective healthcare systems. Typically, cantonal health authorities are tasked with enforcing both local and national health laws. In this system, various regulatory and enforcement bodies have jurisdiction over the digital health sector:

At the federal level:

- Swissmedic: This authority is responsible for the authorisation and supervision of therapeutic products. Swissmedic oversees clinical trials for medical devices and conducts market surveillance.
- Federal Office of Public Health (FOPH): Inter alia, the FOPH handles issues related to reimbursement by compulsory health insurance for medical devices used in therapeutic settings. It also enforces transparency provisions.
- Federal Data Protection and Information Commissioner: Responsible for supervising compliance with federal data protection legislation, this office oversees data processing by federal bodies and private parties.

At the cantonal level:

- Cantonal health authorities: These entities oversee medical professional practice and enforce professional licensing requirements. They are responsible for implementing and enforcing both cantonal and national health laws, including regulations governing digital health technologies impacting professional practice, such as telemedical service platforms.
- Regional ethics committees: Alongside Swissmedic, these committees authorise certain categories of human clinical trials with medical devices under the Swiss Clinical Trials Ordinance.
- Entities designated as 'public bodies' at the cantonal level are governed by cantonal data protection laws and are monitored by the respective cantonal data protection authorities. Many healthcare organisations fall into the category of 'public bodies.'

Law stated - 1 March 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

There is no official authorisation process for medical devices. Digital health products categorised as medical devices unlike pharmaceuticals, do not undergo an official

authorisation process. Switzerland aligns with the European Union's (EU) compliance assessment and certification system for these devices through bilateral agreements. Evaluation of adherence to globally accepted standards is carried out by private organisations. Medical devices are classified into different risk categories, each requiring specific assessment procedures. The CE label, obtained through compliance assessment, allows these devices to be marketed in the EU and, through unilateral recognition, in Switzerland as well. The registration of economic operators and medical devices, including in vitro diagnostic medical devices (unique device identification, UDI), is directly managed by Swissmedic. Manufacturers must comply not only with the device registration criteria outlined in the MedDO and the IvDO but also with the responsibilities and procedures outlined in articles 27 and 29, and Annex VI of the EU Medical Device Regulation and articles 24 and 26, and Annex VI of the EU In Vitro Diagnostic Medical Devices Regulation. These articles will be incorporated into the MedDO and IvDO at a later stage, as the necessary database for this purpose needs to be established first.

Clinical investigations with medical devices, as defined the MedDO, refer to systematic studies involving human subjects to evaluate device safety or performance.

- Authorisation for pre-market investigations requires approval from both Swissmedic and the relevant cantonal ethics committee. Applications and subsequent submissions must be simultaneously sent to Swissmedic and the ethics committee. Swissmedic can grant authorisation only if the ethics committee has approved the trial documentation.
- Post-market clinical investigations solely require approval from the cantonal ethics committee and do not necessitate submission to Swissmedic.

Healthcare professionals engaged in delivering digital health services may need professional licences from relevant health authorities, based on the nature of the service provided.

Law stated - 1 March 2024

Soft law and guidance

9 | Is there any notable 'soft' law or guidance governing digital health?

On 26 May 2021, Swissmedic released a guidance document regarding standalone medical device software, which encompasses applications installed on wearable devices (Information Sheet on Medical Device Software). The document also provided illustrations of non-medical software. Swissmedic refers to the MDR guidance MDCG 2019-11, issued by the EU Medical Device Coordination Group.

In April 2022, the Swiss Competence and Coordination Centre of the Confederation and the Cantons (eHealth Suisse) released the 'Guide for App Developers, Manufacturers, and Distributors,' along with accompanying checklists. This resource aims to assist in the differentiation between 'lifestyle/wellness' products and medical devices.

Law stated - 1 March 2024

Liability regimes

10 What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

Swiss legislation does not include specific liability regulations pertaining to digital health. Instead, general civil liability principles are applicable, notably tortious liability, contractual liability and product liability.

Product safety regulations, which encompass digital health products, establish a standard of strict liability. Accordingly, the manufacturer bears responsibility for any instances of death, personal injury or property damage resulting from product defects. The scope of manufacturer, as defined by the Product Safety Act, extends to individuals claiming manufacturer status or whose name or trademark appears on a product. Additionally, those importing products for resale, rental or other commercial purposes are also regarded as manufacturers.

While product safety regulations are subject to the principle of territoriality, the question of applicable private law claims in cross-border situations is governed by conflict of laws.

Law stated - 1 March 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

Health data allows inferences about an individual's physical or mental health status. According to the Federal Act on Data Protection (FADP) and its accompanying Data Protection Ordinance (DPO), health data is considered sensitive personal data. Sensitive personal data includes genetic and biometric data that can unequivocally identify individuals. Anonymised data refers to information that, after an irreversible process, cannot be linked to a specific individual without disproportionate effort.

Various federal laws and regulations, such as the Human Research Act (HRA) govern the processing of health data. Anonymised health-related data, according to the HRA, is health data that cannot (without disproportionate effort) be traced to a specific person.

Law stated - 1 March 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Health data in Switzerland benefits from a higher level of protection than regular personal data as it is considered sensitive personal data under the FADP and DPO. This includes:

- Extensive processing of health data may potentially pose a significant risk to an individual's identity or basic rights, necessitating the completion of a data protection impact assessment (DPIA). Should the DPIA reveal that the intended processing could still present a high level of risk despite any precautionary measures, consultation with the Federal Data Protection and Information Commissioner (FDPIC) is mandatory before proceeding with such processing (see the FDPIC's 'Factsheet on the data protection impact assessment (DPIA) in accordance with articles 22 and 23 FADP').
- If sensitive personal data is processed automatically on a broad scale or if high-risk profiling is carried out and the preventive measures cannot guarantee data protection, the private controller and its private processor must at least record the storage, alteration, reading, disclosure, deletion and destruction of the data.
- The private controller and its private processor must draw up a processing policy for automated processing if they process sensitive personal data on a broad scale.

In practice, it is important to keep in mind that healthcare providers (HCPs) and healthcare organisations (HCOs) are bound by professional and/or official confidentiality requirements. Revealing confidential information, such as patients' personal health data, to third parties is not allowed unless legally mandated, permitted, or with the informed consent of the patient. However, sharing such information with auxiliary personnel is allowed. The issue of whether IT service providers, including those from foreign countries, can be considered auxiliary personnel under official confidentiality was examined in an expert report dated 16 September 2021, focusing on the use of cloud services by the city of Zurich. It was affirmed that outsourcing is not unlawful when carried out appropriately. This entails that the IT service provider must function in a subordinate role as an auxiliary.

A specific regulation is the HRA, which applies to research concerning human diseases and concerning the structure and function of the human body. The HRA – supplemented by the general principles of the FDPA – provides a general framework for health data used in research projects. The HRA distinguishes between two main types of projects: primary and secondary research. Primary research is the collection of data or biological material directly related to a research project. Secondary research is based on the re-use of data. The HRA is supplemented by several ordinances (Human Research Ordinance (HRO); the Clinical Trials Ordinance (ClinO) and the Ordinance on Clinical Trials with Medical Devices in particular), as well as by several laws or special provisions regulating certain specific aspects.

Law stated - 1 March 2024

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

Truly anonymised health data is not considered personal data. General data protection laws do not apply to such data. The process of anonymising health data itself is subject to relevant data protection rules. Transparent information must therefore be provided about the implementation and purpose (in particular, secondary use) of anonymisation (principle of transparency and purpose limitation). This is usually done in a privacy notice.

The HRA does not apply to research that involves anonymously collected or anonymised health-related data. As already mentioned, this anonymisation process is itself a data processing operation to which the principles of the FADP apply. The HRA does, however, regulate the anonymisation of genetic data for research purposes. Genetic data may be anonymised for research purposes if the person concerned or the legal representative or next of kin has been informed in advance and has not dissented to anonymisation, with the HRO regulating the specifics of the anonymisation.

Law stated - 1 March 2024

Enforcement

14 How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The FDPIC is designated to oversee federal entities, provide guidance to private entities, and enforce federal data protection legislation. Cantonal 'public bodies' are governed by cantonal data protection regulations and are supervised by cantonal data protection authorities. Many HCOs fall under the category of 'public bodies'. These authorities' jurisdiction, resources and determination are not equivalent to those of their European counterparts.

Violations may result in sanctions for the company as well as fines for natural persons. The authorities may conduct investigations or issue orders to restrict, amend or cease processing. The disclosure of data in the context of professional secrecy may result in additional sanctions. Fines (up to 250,000 Swiss francs) may be imposed on persons responsible for an offence. A criminal investigation is possible, and the offence may be recorded in the criminal register. In contrast to the regulation under the General Data Protection Regulation, only certain offences are punishable by law, and even these are only punishable if committed intentionally.

Significant recent activities of the FDPIC concerning health data include:

- In 2022, the FDPIC conducted a fact-finding investigation into the National Organ Donor Register, which was operated by the Swisstransplant Foundation. The FDPIC found the online authentication to be deficient.
- In 2022, the FDPIC opened a procedure to clarify the facts regarding the breast implant register operated by Swiss Plastic Surgery. Its purpose is to record all plastic surgery procedures in connection with breast implants and any difficulties that arise during these operations. The investigation was opened after the FDPIC was notified of an IT design error in the register. As a result of this error, random persons were able to gain access to patients' files in just a few steps. In addition to personal details

(surname, first name, date of birth, etc), detailed medical data on the operation could also be viewed. The register has been taken offline for the time being.

Law stated - 1 March 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

Switzerland has not implemented any comprehensive cybersecurity legislation thus far, nor are there intentions to address the issue comprehensively through a specialised legal framework.

The only clear exception is the Information Security Act (ISA), which came into effect on 1 January 2024, together with its four implementing ordinances. The ISA governs the structuring of the federal administration in terms of safeguarding against cyber risks. The ISA establishes a competence hub – the National Cyber Security Centre (NCSC) – and addresses various compliance requirements for external service providers engaging with the federal administration.

This legislative package does not include the amendments to the ISA, which were introduced during the legislative process and provide for a reporting obligation for cyberattacks on critical infrastructure. According to this, operators of critical infrastructures must report cyber-attacks to the NCSC within 24 hours under certain circumstances. Parliament adopted the amending provisions to the ISA on 29 September 2023. The corresponding ordinance provisions are currently being drafted. The provisions on the reporting obligation will come into force on 1 January 2025. The list of operators of critical infrastructures includes:

- Healthcare facilities on the cantonal hospital lists (in addition to hospitals, also maternity centres and nursing homes);
- medical laboratories with a licence under the Epidemics Act;
- companies that manufacture, place on the market or import medicinal products;
- social insurers;
- manufacturers of hardware or software whose products are used by critical infrastructures and have remote maintenance access or are used to control and monitor operational systems and processes or to ensure public safety (examples include laboratory equipment, eg, automated microscopes or analytical tools).

Data protection legislation is central to cybersecurity for digital health offerings. The FADP governs personal data protection and data security, which is a fundamental aspect of cybersecurity in Switzerland. Data security covers all measures taken to ensure the confidentiality, integrity and availability of data. The legislature adhered to a 'technologically neutral' stance. Controllers and processors must take 'appropriate technical and organisational measures' to ensure data security commensurate with the risk. The greater the risk of a breach of data security, the higher the requirements for the measures to be taken. The FADP provides two tools to assist data controllers and help them

meet their obligations. These aids enable compliance with data protection requirements and offer other advantages:

- Codes of conduct (article 11 FADP, article 12 DPO): These are codes of good practice in data protection, developed by professional, sectoral or economic associations whose rules enable them to defend the interests of their members. These associations can submit their code to the FDPIC, which will publish an opinion.
- Certifications (article 13 FADP, Ordinance on Data Protection Certification): Software and systems suppliers, as well as data controllers and their subcontractors, may have their products certified by an independent approved body. These certifications demonstrate that they meet the requirements of the FADP.

In addition to these frameworks, there are additional rules and requirements for regulated industries, including in the health space (eg, article 74 MedDO, article 51 paragraph 2 of the Medicinal Products Ordinance (VAM); article 12 of Ordinance on the Electronic Patient Record).

Relevant guidelines include:

- In January 2024, the FDPIC published its Guide to Technical and Organisational Data Protection Measures (TOM). In this guide, the FDPIC refers to the Federal Office for National Economic Supply (FONES)'s minimum standar d for improving 'ICT resilience'. It is aimed in particular at operators of critical infrastructures but is basically applicable for any company or organisation and freely available. For medical device software, Swissmedic refers to EU Medical Device Coordination Group 2019-16 Cybersecurity for medical devices.
- There are numerous recommendations aimed primarily at the federal administration.
- The NCSC issued 'Recommendations on cybersecurity in the healthcare sector' in 2022.
- Certain cantonal regulators have issued comprehensive guidelines regarding the use of cloud services by 'public bodies'. They mainly contain requirements regarding data security.

Law stated - 1 March 2024

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Raw data is not necessarily anonymised by definition. Raw data can include personally identifiable (health) information if it has not undergone anonymisation processes and thus constitutes (sensitive) personal data under the FDAP. The already discussed obligations apply, with the above-mentioned guidelines to be considered. The NCSC's

'Recommendations on cybersecurity in the healthcare sector' in 2022 are of specific interest; they include patch and lifecycle management, timely monitoring of log data and the blocking of risky email attachments.

Anonymised health data, however, has already been processed to remove any identifiable information and thus does no longer constitute sensitive personal data under the FDAP. As discussed above, the process of anonymising health data itself is subject to relevant data protection rules (in particular, principle of transparency and purpose limitation).

Under the HRA, further use of genetic and non-genetic health related personal data for research purposes is specifically regulated. The HRA is based on the principle of informed consent: as a general rule, a person – and thus their data – can only be involved in a human research project if that person understands the process, the risks and the stakes, and on that basis give their consent. The HRA applies this principle to varying degrees depending on the type of project.

Law stated - 1 March 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Software itself cannot be patented in Switzerland, but inventions with a technical implementation may be eligible for patent protection. Switzerland is party to the European Patent Convention.

The allocation of inventions and creative works produced by AI-based technologies remains unresolved. Similar to the stance of the European Patent Office, most legal scholars contend that inventorship in patent law and authorship in copyright law are limited to natural persons.

Under Swiss contract laws, designs and inventions conceived or realised during the fulfilment of an employment contract are the property of the employer. A similar provision exists for computer programs protected by copyrights according to the Copyright Act .

Law stated - 1 March 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

Switzerland, as a member of the European Patent Convention, primarily relies on the European Patent Office (EPO) for patent grants. While patent applications can also be filed directly with the Federal Institute of Intellectual Property (FIIP) in Switzerland, Swiss national patents are granted without undergoing novelty and inventive step examinations

under current regulations. There are no specific prosecution procedures for digital health technologies before either the FIIP or the EPO.

Law stated - 1 March 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Under Swiss legislation, computer programs can be protected by copyrights that do not require registration. Unlike in some other jurisdictions, the commercial intellectual property rights to these programs can be freely transferred. It is generally accepted in doctrine that associated moral rights, such as the right to be credited as the author, cannot be transferred but can be waived. There is also an argument that these rights can be exercised by third parties.

Swiss legislation does not address the ownership of copyrighted works produced by employees, except in the case of software copyrights. Consequently, in the absence of contractual clauses, the default rule is that the author of the work, typically the employee, retains the copyright.

Although they are not considered standalone intellectual property rights in Switzerland due to their non-absolute nature, trade secrets and know-how play a crucial role in digital health offerings, similar to other technology sectors.

Trademark protection in Switzerland necessitates registering the symbol with the FIIP.

Law stated - 1 March 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

Swiss law does not impose specific formalities for licensing intellectual property (IP) rights. However, it is common practice and recommended to formalise licensing arrangements through a written agreement and to register the licence. Without such formalities, a licensee may be unable to enforce their licence rights against a third party who acquires the IP rights in question in good faith.

Due to the constraints set by intellectual property laws on collaborative inventions and creative works, contractual agreements frequently govern cross-licensing of background intellectual property rights, as well as the distribution of ownership in foreground intellectual property. Decisions regarding intellectual property allocation should not solely rely on legal counsel, but should involve business engagement and alignment with the broader strategies of the parties.

Law stated - 1 March 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

Enforcing IP rights in digital health technologies follows standard enforcement procedures. Patent infringement and validity cases are initially adjudicated by the Federal Patent Court, which has jurisdiction across the country. Non-patent IP disputes are initially heard by the High Court or Appeals Court of the relevant canton. The Federal Supreme Court serves as the appellate instance for all IP proceedings.

In a recent case before the Federal Supreme Court involving a patent for a ventilator used in intensive care, the court had to determine whether a unique feature of the invention, namely, an animated representation of the ventilated lung displayed on a screen, contributes to solving a technical problem and thus affects the inventive step. The Court ruled in favour of the patent holder.

Law stated - 1 March 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

The Unfair Competition Act (UCA) governing advertising in Switzerland extends to digital health products and services. Misleading advertising is forbidden. Comparative advertising is allowed within Swiss law, provided it is accurate, not deceptive, non-damaging or imitative. Additionally, it must not exploit the reputation of a competitor's trademark.

Regarding advertising and marketing digital health services, regulatory requirements vary depending on each case.

Generally, providing general health information based on predefined references is not specifically regulated in Switzerland. However, offering individual medical advice is restricted to licensed medical professionals registered with the Swiss Register of Medical Professionals (MedReg). Medical professionals must comply with their professional (- Medical Professions Act (MedBG)) and ethical advertising regulations.

Advertising for medical devices must adhere to the advertising rules of the Medical Devices Ordinance. Statements regarding the use, performance and effectiveness of medical devices intended for direct use by or dispensing to the public must align with the product information. Advertising directed at the general public is prohibited for medical devices requiring a medical prescription or exclusively intended for professional use.

Law stated - 1 March 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

Contracts can be established electronically, necessitating mutual agreement between parties on the essential elements of the contract. The acceptance of an offer must mirror the terms of the offer, ensuring customers are fully informed about the product and price.

The UCA outlines obligations for companies offering goods or services online. These include:

- disclosing full identity and contact details, including an email address, in a clear manner;
- detailing the technical steps required to complete the transaction, such as a step-by-step purchase procedure;
- providing the opportunity and means to correct input errors before finalising the order; and
- promptly confirming the order through electronic communication, such as a confirmation email.

The Price Disclosure Ordinance must also be observed.

Law stated - 1 March 2024

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Basic health insurance is mandatory under the Health Insurance Act. It offers the same range of services and benefits to all insured people. Supplementary insurance is optional and subject to the Insurance Contracts Act, covering a higher level of comfort or additional services and benefits.

Typically, mandatory health insurance extends coverage to all treatments administered by physicians. This encompasses services prescribed by physicians and administered by other healthcare professionals, along with examinations ordered by a physician. TARMED is the applicable tariff for outpatient services of physicians (to be modernised after almost 20 years; related negotiations are ongoing). SwissDRG (a flat rate tariff) is the tariff system that regulates the remuneration for services in inpatient acute care.

Medical devices, medications, laboratory tests, aids, dental procedures and maternity or preventive healthcare prescribed by medical professionals are specified in comprehensive positive lists. Any services or products not listed are not covered by compulsory health insurance and do not require reimbursement, following a closed catalogue system. The

lists are established by the Federal Office of Public Health (FOPH) and include tariffs, rates and maximum reimbursement levels:

- provisions on the service obligation and the scope of coverage in the case of aids and devices for examination or treatment (List of Aids and Devices) used;
- list of analyses with tariff (Analysis List);
- list of pharmaceutical specialities and assembled medicines with prices (Specialities List); and
- list of products, active ingredients and additives used in the formula with tariff (List of Medicines).

Digital applications that are used solely to support the activities of healthcare professionals (eg, reading and analysing data or controlling a device) in the outpatient sector are reimbursed as part of the overhead costs included in TARMED. Only if they are genuine additional services (this mainly concerns so-called innovative additional medical services) are they reimbursed separately (ie, through supplementary insurance).

Digital health applications that are used by patients themselves can be linked to devices for monitoring health status, which serve to alert and/or transmit health data to a monitoring centre. There are also software apps for medical purposes for use by patients or carers. These are categorised as aids and devices and are only covered by compulsory health insurance if listed in the List of Aids and Devices.

In 2022, the FOPH published the 'Fact sheet on the reimbursement of digital health applications under compu
lsory healthcare insurance'.

Law stated - 1 March 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

On 26 May 2021, the updated Medical Devices Ordinance (MedDO) came into effect, followed by the introduction of the new Ordnance on In Vitro Medical Diagnostic Devices on 26 May 2022. These changes were aimed at aligning Switzerland's regulations with EU Regulations (EU) 2017/745 (MDR) and (EU) 2017/746. Under previous regulations (the European Medical Device Directive and the former Swiss MedDO), medical devices placed on the Swiss market could also be sold in Europe, and vice versa, due to the mutual recognition agreement (MRA). However, the MRA has not been updated to reflect the new regulations. As a result, Switzerland is now considered a third country under the MDR, leading to the cessation of mutual recognition. The third-country status significantly impacts market surveillance in Switzerland. With Swissmedic losing access to EUDAMED, manufacturers, authorised representatives and importers must register with Swissmedic

to obtain a Swiss Single Registration Number, similar to the SRN used in Europe. This is essential for establishing a market surveillance system in Switzerland. Additionally, devices will need to be registered in swissdamed, the Swiss Database on Medical Devices, with details and deadlines for registration expected to be determined in the future.

On 27 April 2022, the Federal Council announced to the public that the Electronic Patient Record (EPR) would undergo further development. It is intended to be integrated as a component of compulsory health insurance. All healthcare providers operating in outpatient settings will be required to maintain an EPR. Additionally, the Federal Council intends to grant access to research endeavours with the consent of individuals involved. Furthermore, there are plans to utilise the technical framework of the EPR for supplementary services (for more information regarding the further development of the EPR, see here). At its meeting on 28 June 2023, the Federal Council submitted the proposal for the comprehensive revision of the Federal Act on the Electronic Patient Record (EPRA) for consultation. The consultation on the draft of the comprehensive revision of the EPRA lasted from 28 June to 19 October 2023. It will take several years for the amendments to come into force.

Law stated - 1 March 2024

Anne-Catherine Cardinaux anne.cardinaux@walderwyss.com

Walder Wyss Ltd

Thailand

Peerapan Tungsuwan, **Nont Horayangura**, **Panyavith Preechabhan-**
, **Praween Chantanakomes**
Baker McKenzie

Summary

UPDATES AND TRENDS

Recent developments

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

Key players include:

- the Ministry of Public Health (MOPH);
- the Office of the National Broadcasting and Telecommunications Commission;
- public medical schools and private hospitals;
- the Medical Council of Thailand;
- the Pharmacy Council of Thailand;
- the Food and Drug Administration (FDA);
- the Ministry of Higher Education, Science, Research and Innovation; and
- the National Innovation Agency (Public Organisation).

There is a clear trend of new players entering the healthcare space, from tech companies to large conglomerates diversifying their businesses and portfolios. In Thailand, as in other countries in Asia, large conglomerates have begun to explore investment opportunities in the healthcare space whether organically (eg, by building on their existing technology and expanding their current product offerings into healthcare) or through mergers and acquisitions, in the interests of diversifying their business, and with some companies positioning healthcare as its strategic growth initiative.

After the covid-19 pandemic, the awareness regarding the importance of digital health tools has been substantially increased. It has also accelerated digital health trends, particularly the adoption of telemedicine in Thailand. Since 2020, there have been rapid developments on the legal and regulatory front in three main areas, namely:

- the Notification of the Medical Council of Thailand No. 54/2563 regarding Telemedicine and Online Clinical Practice Guidelines, effective on 20 October 2020 (the Telemedicine Guidelines); and
- the Notification regarding Standards of Telemedicine Services Provided by Medical Facilities issued by the MOPH, effective on 2 February 2021 (the MOPH Notification).

With respect to telepharmacy services:

- the Regulations of the Pharmacy Council of Thailand regarding Restrictions and Conditions for the Undertaking of Pharmaceutical Profession (No. 4), BE 2565 (2022), effective on 25 August 2022;
- the Notification of the Pharmacy Council of Thailand No. 62/2565 (2022) regarding Guidelines on the Provision of Telepharmacy Services, effective on 29 January 2023; and

- the Notification of the Pharmacy Council of Thailand No. 91/2565 regarding Criteria, Procedures and Conditions for the Approval of Application for the Provision of Telepharmacy Services, effective on 8 November 2022 (collectively, the Telepharmacy Guidelines).

Law stated - 16 February 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

There has been increasing focus on the part of the government to promote the adoption of digital health technology in line with the Thailand 4.0 policy, an industrial policy unveiled by the Thai government in May 2016 that aims to transform the economy into a value-based economy defined by innovative technology-based manufacturing and services. There exists room for growth owing to Thailand's geographical location, having gained a reputation in Asia as a medical tourism hub because of its high standard of healthcare infrastructure, qualified healthcare professionals, internationally accredited medical services and affordable prices. In addition, Thailand's significant demographic transformation, with a rapidly growing senior population, offers a significant opportunity for investment in multiple business sectors, including smart electronic devices, hospital management software, health-services software and care robots. The Thai government is also implementing the e-health strategy to improve public health services, such as the telemedicine initiative.

The Thailand Board of Investment continues to offer a number of tax incentives to promote and facilitate investment in the technology industry (including those that are healthcare-related).

Challenges include regulations that are not yet up to speed with tech, such as the physical pharmacy and drug sales requirement. The online sale of drugs – for example, a dangerous drug or drug that has not yet obtained approval for advertisement – is prohibited under the drug law.

Only household drugs specified by the FDA may be sold online, provided that approval for advertisement for the sale of the drug is obtained from the FDA.

Law stated - 16 February 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

A number of business operators in Thailand, including hospitals, continue to invest in digital health; for example, a private hospital has teamed up with a major telecommunication company to launch a 5G network-based mobile app, which provides various digital services

to patients, including telemedicine services for follow-up sessions with doctors. Additionally, the hospital has introduced a cloud-based contact centre system to further facilitate communications between the hospital's personnel and patients.

Law stated - 16 February 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

Marketing authorisation

As healthcare companies are highly regulated, it is important to ensure that the target has materially complied with all applicable laws. For instance, in addition to ensuring that the target has obtained all necessary regulatory approvals such as product registrations, import licences (if it imports products) and sales licences, as applicable, it is also important to verify that the target is compliant with other standards and requirements for the target's operations such as meeting personnel qualifications (eg, for registered pharmacists and relevant physicians).

Compliance

Most physicians in Thailand are also public officials and most likely also work in private hospitals and clinics. Working hours or consultation slots to which they commit with the target digital platform therefore should be reviewed so that they are not repetitive with the relevant hospitals and clinics. There might also be a need to verify that they are allowed under the relevant internal public medical school and private hospital regulations to work on the target digital platform. Any incentives given to physicians for patient referrals must be reviewed to prevent any exposure and reputational damage. In general, it is fair to say that any arrangement, contract or informal relationship that the target platform has with physicians and pharmacists must be closely scrutinised.

Intellectual property

There is a need to understand the ownership or proprietary rights over the platform or copyright on relevant content contained in the platform and its improvement. For example, if the target uses certain technology or Intellectual property (IP) in its business operations, does the target own the technology or IP, or is the technology co-owned with other third parties, such as universities or research organisations? Has the technology been developed by the target or acquired or licensed from another company? It will be necessary to verify the target's rights in each case and ensure that they are duly protected or secured.

Cross-border considerations

If the platform and its technology allow patients who live overseas to access its services, there will be a need to consider the risks and exposure arising from cross-border contracts, such as applicable laws and the implications of the legal requirements of the countries where the patients live.

Law stated - 16 February 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

One of the most common forms of financing for digital health ventures is still private money, such as private equity investment.

There have been discussions regarding a regulatory sandbox as one of the government initiatives to promote the development of a legal framework that will facilitate the development of the digital health space.

Law stated - 16 February 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 What principal legislation governs the digital health sector in your jurisdiction?

There is no bespoke digital health legislation. The key legislation includes:

- the Personal Data Protection Act, BE 2562 (2019);
- the National Health Act, BE 2550 (2007);
- the Electronic Transactions Act, BE 2544 (2001);
- the Drug Act, BE 2510 (1967);
- the Notification regarding Standards of Telemedicine Services Provided by Medical Facilities issued by the Ministry of Public Health (MOPH), effective on 2 February 2021 (the MOPH Notification); and
- notifications and guidelines issued by the Medical Council of Thailand (including, but not limited to, the Notification of the Medical Council of Thailand No. 54/2563 regarding Telemedicine and Online Clinical Practice Guidelines, effective on 20 October 2020 (the Telemedicine Guidelines)) and the Pharmacy Council of Thailand (including, but not limited to, the Regulations of the Pharmacy Council of Thailand regarding Restrictions and Conditions for the Undertaking of Pharmaceutical Profession (No. 4), BE 2565 (2022), effective on 25 August 2022, the Notification of the Pharmacy Council of Thailand No. 62/2565 (2022) regarding Guidelines on the Provision of Telepharmacy Services, effective on 29 January 2023, and the

Notification of the Pharmacy Council of Thailand No. 56/2563 regarding Standards and Procedures for the Provision of Telepharmacy Services, effective on 2 June 2020, and the Notification of the Pharmacy Council of Thailand No. 91/2565 regarding Criteria, Procedures and Conditions for the Approval of Application for the Provision of Telepharmacy Services, effective on 8 November 2022 (collectively, the Telepharmacy Guidelines)) for doctors and pharmacists to follow.

Law stated - 16 February 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

The notable regulatory and enforcement bodies are:

- the Ministry of Digital Economy and Society;
- the MOPH;
- the Food and Drug Administration (which is a government entity under the MOPH); and
- the Personal Data Protection Committee (PDPC).

Law stated - 16 February 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

There is no specific licence required for the provision of digital health products and services. However, specific laws may apply, depending on the type of digital health products or services. For example, digital products that are deemed to be medical devices may be subject to the licensing requirements under the Medical Device Act, BE 2551 (2008).

Additionally, the MOPH Notification provides that a medical facility wishing to provide telemedicine services is required to submit a supplement service application form in respect of the telemedicine service. Moreover, a medical facility must comply with the requirements imposed under the MOPH Notification (eg, a medical facility must also ensure the availability of a sufficient number of professionals to provide the telemedicine service without disrupting the medical facility's main services).

Furthermore, digital health products or services that are considered a digital platform service under the Royal Decree on the Supervision of Digital Platform Services Subject to Prior Notification B.E. 2565 (2022) (ie, intermediary platform for the purpose of generating electronic transactions) may also subject to notification requirements thereunder prior to the operation of the service.

Law stated - 16 February 2024

Soft law and guidance

9 | Is there any notable 'soft' law or guidance governing digital health?

According to the Telemedicine Guidelines, the doctor who is the service provider must only provide the service through licensed medical facilities. Medical operations must be performed in accordance with the main requirements as follows:

- both the service provider and the service recipient should be aware of, and must acknowledge, the medical facts as stated in clause 7 of the Declaration of Patient's Rights and Responsibilities, issued on 12 August 2015, and other medical facts that may subsequently arise (eg, screening, diagnosis and follow-ups may have variations owing to limitations of technology and other uncontrollable factors, and healthcare personnel have the right to select the type of treatment according to their knowledge, capability and limitations, including consultations and transfers when deemed appropriate for the patients' highest benefits);
- both the service provider and the service recipient should be aware of, and must acknowledge, the fact that only certain diseases or conditions are suitable for the use of telemedicine;
- both the service provider and the service recipient should be aware of, and must acknowledge, the technological and electronic restrictions, including the recipient's right to refuse the use of medicine;
- the service provider must comply with the Professional Standards for Medical Practitioners of the Medical Council of Thailand, BE 2555 (2012) – for example, having scientific knowledge of medicine, communication and interpersonal skills as per the standards required, and being able to provide patient care as per the standards required; and
- the use of tools, computer programs or artificial intelligence jointly with telemedicine is also required to be in accordance with the relevant laws (eg, the medical device and drug laws).

Also, there are the Telepharmacy Guidelines, which provide guidelines for dispensing drugs to a patient at a distance via online means. Two key scenarios under the Telepharmacy Guidelines are dispensing prescription drugs and non-prescription drugs.

Dispensing non-prescription drugs can be done with certain conditions including, but not limited to, obtaining consent regarding the patient's health data, and preparing and maintaining the patient profile and medical records. Similar conditions also apply to dispensing prescription drugs with an additional condition that the patient must provide a relevant prescription for receiving such prescription drugs.

Law stated - 16 February 2024

Liability regimes

10 What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

The general tort law is applied. A business operator will be liable if there is damage arising from actions based on wilful misconduct or negligence.

For digital health products, the most restrictive standard that could be applied is provided under the Liability for Injuries from Unsafe Products Act, BE 2551 (2008) (the PL Law). Under the PL Law, even where there is no wilful misconduct or negligence, the business operator may still be liable to the consumer because the law imposes strict liability. A business operator (a manufacturer, importer, seller and person who uses a name, trademark, trade name, mark or statement that would lead to the understanding that he or she is the manufacturer, hirer for manufacture or importer of the product) will also be held jointly liable with other relevant business operators to compensate the injured persons, even if this business operator did not intend to cause injury or was not acting negligently. This may arise from a manufacturing defect, design defect or failure to provide an appropriate warning.

These key liability regimes are also applied to the cross-border provision of digital health products and services. However, they may not have extraterritorial enforcement.

There is no specific law governing malpractice in Thailand. In litigation against hospitals or doctors, patients must base their claims on general law (namely, tort law or contract law (Thai Civil and Commercial Code)). As doctors are required to comply with the Medical Council Regulations on Medical Ethics Preservation, any variation of practice from the code might expose relevant doctors more to liability under tort claims.

Law stated - 16 February 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

Personal health information includes information expressed in the form of documents, files, reports, books, diagrams, maps, drawings, photographs, films, recordings or sounds, recordings made by electronic devices, or any other means that enable recordings to appear concerning the health of an identifiable individual and to include other information, as notified by the Electronic Disclosure Committee. There is currently no specific definition of anonymised health data.

Law stated - 16 February 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

The Personal Data Protection Act, BE 2562 (2019) (the PDPA) imposes more stringent requirements when collecting certain types of personal data that are considered sensitive personal data, for which explicit consent must be obtained from the data subject and where other legal exemptions could not apply. These include data pertaining to, among other things, health data, disability status, genetic data, biometric data or any data that may affect the data subject in the same manner as to be prescribed by the Personal Data Protection Committee. The National Health Act, BE 2550 (2007) also provides that a person's health data is considered confidential personal information. No person can disclose it in such a manner as to cause damage to him or her unless it is done according to the individual's will or is required by a specific law.

Law stated - 16 February 2024

Anonymised health data

13 Is anonymised health data subject to specific regulations or guidelines?

There are no specific regulations or guidelines relating to anonymised health data.

Law stated - 16 February 2024

Enforcement

14 How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The key requirements under the PDPA are, among others, the legal justification for the collection, use and disclosure of personal data (namely, the consent or other legal exemptions or justification), and the notification of the required details under the PDPA to the data subject (namely, a notification of privacy notice). With regard to the legal justification for the collection, use and disclosure of sensitive personal data, which includes health data, the PDPA requires that explicit consent must be obtained from data subjects before or at the time of the collection, use or disclosure of that data, or all three, unless other legal exemptions applicable to sensitive personal data under the PDPA could apply (eg, when the collection, use and disclosure of such health data is for the prevention or suppression of a danger to life, body or health of a person where the data subject is incapable of giving consent for whatever reason).

When consent is required to be obtained under the PDPA, the consent request should be in accordance with the requirements of the PDPA. For example, it should be presented in an easily accessible and intelligible form and style, using clear and plain language. With regard to the notification requirement, a data controller is required to provide a data privacy notice to the data subjects (eg, patients) to inform them of the required details as prescribed

under the PDPA, which includes the purpose of the collection, use or disclosure of the personal data. Apart from the aforementioned key legal requirements, a data controller must ensure that it complies with the other requirements of the PDPA (eg, maintaining appropriate security measures that meet standards as required by laws, data breach notification requirements, cross-border transfer requirements, handling of data subject rights and honouring any agreements with third-party data processors (namely, having in place data processing agreement with data processors)).

Non-compliance with the obligations as prescribed under the PDPA could result in:

- civil liability with punitive damages;
- criminal liability of imprisonment up to one year or a fine up to 1 million baht or both; or
- an administrative penalty of up to 5 million baht.

The PDPA has been in full effect since 1 June 2022.

Law stated - 16 February 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

The PDPA along with the Notification of the Personal Data Protection Committee re: Security Measures for Data Controllers B.E. 2565 (2022) require the implementation of security measures for personal data in order to prevent unauthorised or unlawful loss, access to, use, alteration, amendments or disclosure of personal data. The measures shall include at the minimum administrative, technical and physical safeguards to control access to personal data that must be in accordance with the standards prescribed under the notifications. Under the Cybersecurity Act, BE 2562 (2019) (the Cybersecurity Act), private organisations could be subject to the obligations under the Cybersecurity Act.

As an organisation of critical information infrastructure (the CII Organisations), the main obligations include:

- to prevent, deal with and mitigate risks of cybersecurity (including complying with the code of practice and minimum cybersecurity standards);
- report to the competent authorities any cyber threat;
- conduct a cybersecurity risk assessment; and
- provide names and contact information of the owner or owners, person or persons possessing the computer and person or persons monitoring the computer system, etc.

According to the Notification of the National Cybersecurity Committee regarding Prescribing Criteria and Types of Organisations with Tasks or Services as Critical Information Infrastructure Organisations and Assigning Control and Regulation, BE 2564 (2021) (the CII Notification), it prescribes a list of CII Organisations and relevant regulators

in charge of supervising and regulating the cybersecurity for each type of organisation that is considered a CII Organisation. The brief list of types of organisations that may be deemed CII Organisations include, among others, organisations providing digital health services. Note that the CII Notification empowers the competent regulators to issue a guideline to consider whether or not organisations under such regulators' supervision would be deemed a CII Organisation under the prescribed list of CII Organisations in accordance with the CII Notification and will report to the Office of National Cybersecurity Committee accordingly.

Additionally, a private entity could also be subject to orders from the competent officers under the Cybersecurity Act in general (eg, an order to access computer data, a computer system or other data related to the computer system, seize or freeze a computer, a computer system, or any equipment, etc). The power and authority of relevant competent officers against a private entity will be different depending on the level of a particular cyber threat (eg, non-critical level, critical level and crisis level).

Law stated - 16 February 2024

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

For personal data, the best practice is to ensure that there is a legal justification for the collection, use and disclosure of personal data (eg, obtaining proper consent or relying on other legal exemptions or justification). For the protection of anonymised data and its sharing and management, it is best for the relevant parties to consider having a data-sharing agreement that includes obligations concerning the handling and protection of such shared data.

Law stated - 16 February 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Computer programs are not patentable and are protected by copyright. However, computer-related inventions, including inventions related to software, the series of steps in algorithms, database systems and AI processing, may be patentable, provided they are of 'technical character' in their function and deliver 'technical effect' other than normal interactions between computer programs (software) and computers (hardware) on which they are run.

Copyright belongs to an employee unless the parties agree otherwise. For inventions created by employees, the Thai Patent Act provides that the employer has ownership over

inventions made by its employees during the term of employment, unless the employment agreement provides otherwise. The employee inventor, however, has the right to be named as the inventor in the patent application. It is worth noting that the Thai Patent Act also provides that an employee inventor has the right to receive 'special remuneration' other than his or her regular salary if the employer derives benefits from – or uses the invention when – the patent is granted.

Law stated - 16 February 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

The patent registration procedure in Thailand for digital health technologies is the same as other inventions in other technology areas. There is no fast track for any particular type of technology in Thailand.

When a patent application is filed either via the Paris Convention or the Patent Cooperation Treaty, the patent specification and claims along with formality documents (eg, Power of Attorney and Deed of Assignment) must be submitted in the Thai language. The examiner will conduct a preliminary examination of the patent application, which includes a formality check and examination of the patent eligibility of the invention. Once the patent application passes the preliminary examination, it will be subject to publication. Any person can file an opposition to the patent application within 90 days of the publication date. The patent applicant will have to submit a request for substantive examination within five years of the publication date.

If a corresponding patent application has been filed and granted by either the European Patent Office, Japan Patent Office, United States Patent and Trademark Office, Chinese National Intellectual Property Administration, Korean Intellectual Property Office or Australian Patent Office, the patent application will be subject to a modified substantive examination, meaning that the applicant can amend the Thai pending patent claims to conform with the granted claims of the selected corresponding patent, provided that said amendment does not add new matter to the invention. The examiner will then examine the patent application based on the examination result of the selected corresponding patent. This process could expedite the examination process, and the Thai patent application would be granted in a shorter time.

Law stated - 16 February 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

IP rights in addition to patents subsisting in digital health may include, among others, copyright, trade name, trademark, confidential information and trade secret. The software

technologies involved in digital health, such as applications developed by a creator, as well as the contents or images used in digital health offerings, are protected as copyright. Under the Thai Copyright Act, as copyright subsists in the work upon creation, it does not require registration. A copyright owner may have the copyrighted work recorded at the Copyright Office, but this serves only as prima facie evidence of ownership.

The name or brand of a wearable device, application or health service that encourages brand recognition can be protected as a trade name or trademark. While a trade name does not require registration, a trademark must be duly registered with the Trademark Office to be fully protected in Thailand. Although there are registered trademarks in place, if there are any new products or services created that have not been registered, it is advisable to register the trademarks to cover additional products and services to enjoy full protection under the Trademark Act.

In the event that digital health technologies may not be eligible for patent or design protection, or the owner does not wish to disclose it to the public, trade secret protection may be an alternative option. However, not all types of information can be protected as a trade secret. According to the Thai Trade Secret Act, to be protected as a trade secret, the information must not be publicly known, it must have inherent economic value from being kept secret, and appropriate security measures must be taken to keep such information secret. Confidential information, which is not considered a trade secret, may be protected as confidential information under a proper contractual relationship such as a non-disclosure agreement.

Law stated - 16 February 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

As the development of digital health technologies may involve different kinds of IP rights, the practical considerations related to digital health technologies include, among others:

- types of IP rights in digital health technologies;
- ownership of IP rights in each part of digital health technologies (ownership of IP rights belongs to the company, creator, contractor, employer, employee, co-owners, etc);
- licence terms (as digital health technologies consist of various licences; the terms of each licence may vary);
- pending trademark, design or patent applications can be appropriately licensed prior to granting registration;
- IP rights are based on a territorial basis, some of which may have to be registered in the targeted countries within the specific period (namely, within the patent or design's priority claim date) to be protected in such countries;
- scope of the licence (eg, exclusive or non-exclusive, etc);
-

restrictions prohibiting the licensee from doing something, such as sub-license the licensed technology to others; and

- the different legal requirements of IP rights in licensing digital health technologies (eg, licensing of a registered trademark must be in writing and registered with the Trademark Office).

Law stated - 16 February 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

The procedures governing the enforcement of IP rights in digital health technologies depend on the types of IP rights and should be assessed on a case-by-case basis. If the involved parties were able to establish IP rights in a digital health technology, it would ease the enforcement of those IP rights. Enforcement of IP rights in Thailand can be criminal or civil actions, depending on the available legal grounds. In the case of infringement, the rights holder may opt to send a cease-and-desist letter to the infringer and negotiate with the infringer to comply with their demands, proceed with notice and takedown, file a complaint with the police to conduct a criminal police raid, or file a civil or criminal lawsuit with the court.

Based on our experience, we have yet to see notable enforcement action involving digital health technologies in Thailand.

Law stated - 16 February 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

Thailand does not have consolidated legislation regulating advertising and marketing practices. However, the Consumer Protection Act, BE 2522 (1979) (the CPA) is a comprehensive piece of legislation that generally applies to all kinds of commercial media, including billboards, leaflets, newspapers, printed materials, radio, television and online media.

The main advertising restriction under the CPA prescribes that an advertisement must not contain any statement that takes unjust advantage of consumers, or include any statement that may have a harmful impact on society as a whole, regardless of whether the statement regards the origin, condition, quality, appearance, delivery, procurement or application of a product or service.

Statements that have been deemed as taking unjust advantage of consumers or having a harmful impact on society include false or exaggerated statements and statements that may lead to a material misunderstanding concerning the product or service.

Advertisements of drugs and medical devices are subject to, generally speaking, prior approval from the Food and Drug Administration in accordance with the Drug Act, BE 2510 (1967) and the Medical Device Act, BE 2551 (2008). This approval requirement applies to all means of advertisement, including online media. Over-claimed and false or exaggerated statements are prohibited.

Law stated - 16 February 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

E-commerce and online sales in Thailand are generally governed by two laws: the Direct Sales and Direct Marketing Act, BE 2545 (2002) and the Commercial Registration Act, BE 2499 (1956). A direct marketing licence must be obtained from the Office of the Consumer Protection Board, while a commercial registration must be obtained from the Ministry of Commerce prior to the operation of the e-commerce business.

One of the major requirements under the direct marketing law is that the direct marketing business operator must comply with the return and refund policy. According to the law, the customer is entitled to terminate the contract upon expressing his or her intention in writing to the business operator within seven days of the day the customer received the goods or services. Upon the customer's exercise of his or her right, the business operator must refund the customer the full amount of the purchase price of the goods or services within 15 days of the day the business operator received the notice to terminate the contract.

Thai law recognises e-agreements as equivalent to a wet signature and a hard copy document provided that they are reliable and meet the criteria provided by the Electronic Transactions Act, BE 2544 (2001), as amended, which applies to civil and commercial transactions operated by using electronic data. For electronic payments, the electronic payment operator must comply with the Payment Systems Act, BE 2560 (2017) and other relevant regulations.

Law stated - 16 February 2024

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Many insurance companies have expanded their health insurance policies to doctors' fees and drugs available from e-pharmacies. The relevant government agency, the National

Health Security Office, has issued guidelines that allow for reimbursements to patients who are entitled to the Universal Coverage Scheme. The Universal Coverage Scheme covers broad claims, for example, general diseases, costly diseases, dental surgery, and certain drugs and medical supplies. It also covers limited claims for telemedicine.

Law stated - 16 February 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

Thailand now has specific regulations and guidelines on the provision of telemedicine and telepharmacy services (including the Notification of the Medical Council of Thailand No. 54/2563 regarding Telemedicine and Online Clinical Practice Guidelines, effective on 20 October 2020, the Regulations of the Pharmacy Council of Thailand regarding Restrictions and Conditions for the Undertaking of Pharmaceutical Profession (No. 4), BE 2565 (2022), effective on 25 August 2022, the Notification of the Pharmacy Council of Thailand No. 62/2565 (2022) regarding Guidelines on the Provision of Telepharmacy Services, effective on 29 January 2023, and the Notification of the Pharmacy Council of Thailand No. 91/2565 regarding Criteria, Procedures and Conditions for the Approval of Application for the Provision of Telepharmacy Services, effective on 8 November 2022).

The Notification of the Pharmacy Council of Thailand No. 62/2565 (2022) regarding Guidelines on the Provision of Telepharmacy Services provides specific requirements for the provision of telepharmacy services (this includes the requirement that telepharmacy services must be provided via an application that meets certain criteria (eg, having in place systems to maintain the patients' digital health data and having in place features for video call, voice call and messaging)).

However, there remain a number of challenges that may still have an impact on the full development of the digital health sector in Thailand, specifically from a regulatory perspective (eg, laws restricting the online sales of drugs, etc).

Law stated - 16 February 2024

Peerapan Tungsuwan peerapan.tungsuwan@bakermckenzie.com
Nont Horayangura Nont.Horayangura@bakermckenzie.com
Panyavith Preechabhan panyavith.preechabhan @bakermckenzie.com
Praween Chantanakomes praween.chantanakomes@bakermckenzie.com

Baker McKenzie

USA

Abeba Habtemariam, **Nancy L Perkins**, **Chris Anderson**, **Monique Nolan**, **Alice Ho**
Arnold & Porter

Summary

UPDATES AND TRENDS

Recent developments

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

The key players in the growing digital health marketplace include traditional medical device manufacturers, pharmaceutical companies, health systems and other clinical providers, and digital health-focused technology startups, as well as consumer health firms focused on general wellness and 'femtech' tools, clinical research organisations and venture capital, private equity and strategic investors. Some of the largest publicly traded companies (Amazon, Alphabet, Apple, IBM, Microsoft) are increasingly devoting significant resources to this sector even if outside of their core competencies. The market growth is fuelled by mHealth, wearable devices, remote monitoring and the ensuing large data sets leveraging artificial intelligence (AI) and machine-learning (ML) to drive precision, efficiency and convenience in the delivery of care. For example, a number of healthcare systems and vendors have increasingly sought strategic partnerships with AI companies to streamline healthcare services, reduce the burden on providers and improve patients' experiences.

Other prominent areas of digital health innovation include clinical decision support tools, medical imaging, digital therapeutics, robotics, remote data acquisition technologies, direct-to-consumer wellness and diagnostic lab testing services, and augmented reality and virtual reality technologies. Among theMedical Futurist's Top 100 digital health and AI companies to watch in 2024 are CELLINK, FabRx, Medivis, CloudMedX, Corti.AI, DeepMind, Enlitic, Ada Health, Arterys and Idoven.

Law stated - 16 February 2024

Investment climate

2 How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

Surprisingly, given the promise of advances in this space, the venture funding for digital health technologies was significantly slower in 2023 than in recent years, continuing the trajectory that started in 2022. As reported by Rock Health, in 2023, digital health startups brought in US$10.7 billion across 492 deals, representing the lowest amount of capital invested in the digital health sector since 2019, and there were no initial public offerings (IPOs). While Waystar Holding Corp, a digital health company that facilitated over US$4 billion in healthcare payment transactions last year by assisting hospitals and clinics in managing their finances, made its IPO filing public in mid-October after filing confidentially in August, it was announced on 1 November that Waystar would delay its IPO until 2024 to ride out the market volatility and avoid a similar fate to other high-profile companies that recently went public only to trade below their IPO prices. In light of the historically high interest rates and their effect on private investors, digital health startups looking for new capital are more frequently turning to larger strategic investors with the ability to fund from their balance sheet. During the first half of 2023, 71 per cent o[1] f digital health deals

were done by repeat digital health investors, signalling that the digital health market is increasingly controlled by a smaller, more powerful group of investors. For example, recent data shows that Alphabet, Microsoft and Tencent are parties to over 70 per cent of reported digital health agreements.

Law stated - 16 February 2024

Recent deals

3 What are the most notable recent deals in the digital health sector in your jurisdiction?

The first half of 2023 featured several large deals for this sector. Notably, Strive Health, Arcadia and Vytalize Health each secured substantial funding in the value-based care enablement space. Additionally, nonclinical workflow and practice management companies such as Shiftkey, ShiftMed and MedShift, along with at-home care providers such as Author Health and Monogram Health, attracted significant investments. Hospitals also continued to announce partnerships leveraging AI capabilities. On 2 August 2023, Duke Health announced it will use its partnership with Microsoft to explore and develop new mechanisms of applying Microsoft's generative AI and cloud technologies (called Nuance) to its research and operations and plans to use Nuance to optimise clinic schedules and attempt to predict which patients are most likely to be no-shows for their appointments. Likewise, Aegis Ventures and Northwell Holdings, the for-profit arm of Northwell Health, launched Optain, a digital healthcare company that will use AI-backed retinal imaging to attempt to detect early signs of disease. Specifically, Optain will provide screening for diabetic retinopathy, age-related macular degeneration and glaucoma with the goal of reducing reactive care with increased preventative care. The launch of Optain is part of a growing global trend of venture capital firms partnering with health systems to drive direct-to-patient digital health companies.

Law stated - 16 February 2024

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

The specific diligence issues that should be addressed will turn on the nature and structure of the digital health transaction and the types of products, services or offerings involved. A few examples of core diligence issues that should be addressed include the following:

- the regulatory status of the products involved, including whether any of the products are medical devices. For devices, diligence should ensure compliance with applicable Food and Drug Administration requirements;
- compliance with any applicable state licensing and registration requirements;
- privacy and data collection, protection and security-related considerations;

- cybersecurity and IT compliance considerations;
- coverage and reimbursement considerations (if applicable);
- compliance with any fraud and abuse laws applicable to the specific target products and related services or arrangements;
- compliance with any applicable corporate practice of medicine laws;
- intellectual property rights considerations; and
- product liability considerations.

This list is by no means exhaustive, and provides just a few examples of key diligence areas to consider in digital health-focused transactions. Due to the evolving nature of laws governing digital health technologies at both the federal and state level, a robust diligence review of these areas is imperative.

Law stated - 16 February 2024

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

Digital health ventures avail themselves of all of the usual early-stage funding strategies with venture funding typically playing a crucial role. However, as venture funding for digital health experienced a decline in 2023, founders increasingly turned to alternative financing structures. For example, a number of digital health startups that previously raised early-stage rounds opted for unlabelled funding deals to avoid valuation shortfalls or disclosing weak rounds of investments, extension rounds or silent deals from existing investors to buy time. Unlabelled funding deals where capital raises fail to have a Series A or similar status, comprised a staggering 41 per cent of digital health funding deals during the early part of 2023. This is the highest proportion of unlabelled rises since Rock Health began tracking in 2011. Grants for the development of digital health technology have become increasingly popular among government agencies that promote healthcare research and solutions, such as the National Institutes of Health, the National Institute of Mental Health, the National Institute on Aging and the National Cancer Institute on the heels of the covid-19 pandemic and an aging population that prefers to age in place. These grants, while not of significant dollar value, are nonetheless typically very attractive to founders as they are non-dilutive to the cap table.

Law stated - 16 February 2024

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 What principal legislation governs the digital health sector in your jurisdiction?

Key laws relevant to the digital health sector include, but are not limited to, the Federal Food, Drug, and Cosmetic Act (FDCA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Trade Commission Act (FTC Act), federal fraud and abuse-related laws and various state laws.

For digital health products that meet the definition of a medical device, a principal governing legislation is the FDCA. The FDCA and Food and Drug Administration (FDA)'s implementing regulations set forth requirements intended to help ensure the safety and efficacy of medical devices. Such requirements include ones governing clinical trials and investigational uses, manufacturing facility registrations, marketing authorisations, product labelling and packaging, product promotion and advertising, quality system compliance, cybersecurity, and post-market safety reporting and field actions.

HIPAA and related rules set limits and conditions on the uses and disclosure of protected health information that covered entities and business associates may make without an individual's authorisation. Digital health technologies are also governed by the FTC Act and related Federal Trade Commission (FTC) regulations governing deceptive trade practices, including prohibitions on misleading consumers about what is happening with their health information. Notably, the FTC Act's obligations are not limited to HIPAA-covered entities and business associates. For example, the FTC's Health Breach Notification Rule (HBN Rule) applies to certain business entities that are not covered by HIPAA, such as vendors of personal health records (PHR), PHR-related entities and third-party service providers.

In addition, the Office of the National Coordinator for Health Information Technology (ONC) recently issued a rule implementing the electronic health record (EHR) reporting provisions of the 21st Century Cures Act by establishing new certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program. The rule is intended to advance interoperability, improve algorithm transparency, and support the access, exchange and use of electronic health information. While the rule was initially set to go into effect 8 February 2024, the effective date has since been delayed.

Certain digital health arrangements or offerings can also implicate fraud and abuse laws (eg, the Federal False Claims Act, Stark Law, Anti-kickback Statute).

Law stated - 16 February 2024

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

Regulatory and enforcement bodies with jurisdiction over the digital health sector include, but are not limited to, the FDA, FTC, Department of Health and Human Services' Office for Civil Rights (HHS OCR), the Centers for Medicare and Medicaid Services (CMS), ONC, HHS' Office of the Inspector General (OIG), the Department of Justice (DOJ) and state Attorney Generals and regulatory authorities.

The FDA administers the FDCA and has jurisdiction over digital health technologies that meet the definition of a device and certain related entities to varying degrees (eg,

manufacturers, specification developers, labellers, importers, distributors or user facilities). The FTC administers the FTC Act and related regulations relating to deceptive trade practices. This includes investigation and enforcement of the FTC HBN Rule. HHS' OCR is responsible for enforcing the HIPAA privacy and security rules.

Law stated - 16 February 2024

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

Digital health products that meet the definition of a medical device are subject to regulation by the FDA. Under the FDCA definition of 'device', this analysis turns primarily on whether the software is intended for use in the diagnosis, cure, treatment, mitigation or prevention of a disease or other condition. As amended by the 21st Century Cures Act, the FDCA device definition excludes certain categories of low-risk software functions, including:

- certain software functions intended for administrative support of a healthcare facility;
- certain general wellness software functions;
- certain software functions intended to serve as electronic patient records provided specified certification and other criteria are met;
- certain software functions for transferring, storing, converting or displaying medical device data and results; and
- certain clinical decision support software functions intended for healthcare providers (but only if the software meets specified criteria).

Digital heath products that fall under one or more of the above exclusions are not considered medical devices and do not require an FDA device marketing authorisation. Digital health technologies that do not fall under a statutory exclusion should also be evaluated against the FDA's enforcement discretion policies. As articulated in FDA guidances, for certain digital health software functions, the FDA has elected to exercise enforcement discretion not to enforce some or all applicable FDCA requirements. If a digital health product meets the definition of a device and does not fall under an enforcement discretion policy, then understanding whether the product could require marketing authorisation turns on the product's classification. The FDA places devices into one of three classes based on their risk:

- Class I devices generally do not require marketing authorisation but are subject to various general controls.
- Class II devices generally require marketing authorisation through the FDA's premarket notification process (also referred to as '510(k) clearance'). The standard for 510(k) clearance is a demonstration that a device is 'substantially equivalent' to a legally marketed predicate device. Class II devices are subject to general controls and can be subject to additional special controls (eg, performance standards).
-

Class III devices generally require approval through the more rigorous premarket approval application (PMA) process based on clinical studies demonstrating the safety and efficacy of the device for its proposed intended use. Class III devices are subject to general controls and often special controls.

If a proposed novel digital health technology meets the definition of a device but does not fall under an existing classification or lacks an appropriate predicate device, the product is considered a Class III device by default (requiring PMA approval). However, for novel devices that do not pose a high level of risk, sponsors can submit a *de novo* request for classification, asking that the FDA place the device type in Class II or Class I.

With respect to clinical trial authorisations, unless an exemption applies, clinical investigations for investigational devices are subject to the FDA's 21 C.F.R. Part 812 investigational device exemption requirements.

In addition to the above product marketing authorisation requirements, entities involved in the manufacturing of digital health devices (and certain other related entities) are subject to FDA establishment registration requirements. Manufacturers and distributors of digital health devices may also be subject to state-specific registration and licensure requirements.

Law stated - 16 February 2024

Soft law and guidance

9 | Is there any notable 'soft' law or guidance governing digital health?

Various regulatory authorities and other entities have issued guidance governing digital health technologies. For example, the FDA has issued guidance explaining the types of low-risk device software functions for which the agency intends to exercise enforcement discretion, evaluation of when changes to software algorithms may trigger the need for new device marketing authorisations, guiding principles for good machine learning practices, and recommendations for cybersecurity compliance.

Other examples include regulatory authority guidelines pertaining to data security and protecting personal health information (eg, FTC). For a recent example, on 15 February 2024, the National Institute of Standards and Technology issued updated guidance on ensuring the cybersecurity of electronic protected health information under HIPAA. For telemedicine providers, examples of guidelines include those to help minimise enforcement risk outlined in OIG's July 2022 Special Fraud Alert on telemedicine and OIG's telehealth claim risk analysis resources.

Law stated - 16 February 2024

Liability regimes

10 |

> What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

Liability regimes for digital health technologies can include theories rooted in contract, tort and consumer protection. Liability can also stem from violation of various federal and state laws, laws related to protection of personal health information, as well as statutes prohibiting fraud and abuse.

Depending on the state and jurisdiction, tort liability for injuries caused by digital products and services can be imposed under two theories – product or strict liability (which imposes liability for defective products regardless of the defendant's fault) and common law negligence (which imposes liability based on the defendant's fault). Generally, to be held liable under a strict liability theory, the injury must have been caused by a tangible product (as opposed to a service) and must have been caused by a defect in manufacture, design or warning. On the other hand, negligence claims consider whether the defendant breached a duty of care that was owed to the plaintiff.

With respect to tort liability specifically relating to AI used in digital health technologies, there is sparse case law. As explained in a recent policy brief by Stanford University on AI liability risks, few personal injury claims have led to judicial opinions, and in software liability cases that have been decided to date, plaintiffs have grappled with a variety of challenges. Stanford's analysis of cases related to physical injuries from AI and other software found that liability claims generally relate to:

- cases where defects in software used to manage care caused patient harm and patients sued the software developer or hospital for negligently maintaining it;
- cases involving harm that occur after physicians consult software to make patient care decisions and patients sue the developer for erroneous software design or the physician for relying on erroneous software recommendations; and
- cases where software embedded within a device malfunctioned and patients sued physicians or hospitals alleging negligent use, installation or maintenance of the devices.

A trend identified in Stanford's analysis is that plaintiffs struggle to sustain claims when they cannot identify specific design defects in software, and identifying how and why errors occurred can be made challenging by the difficulties in understanding how AI technologies work and produce their outputs.

For certain digital health technologies, the False Claims Act (FCA) and other fraud and abuse laws are also of relevance when analysing liability risks. Under the FCA, it is illegal to submit false or fraudulent claims for payment to the federal government. A powerful tool in the government's efforts to combat healthcare fraud, the FCA's qui tam (or whistle-blower) provisions allow private citizens to bring suit on behalf of the government for violations and receive a portion of the recovery. Cases have been brought under the FCA against various types of digital health companies, with the DOJ showing particular focus on fraud involving telehealth and EHR companies. For example, in June of 2023, the DOJ announced a nationwide law enforcement action that resulted in criminal charges against 11 defendants in connection with the submission of over US$2 billion in fraudulent claims resulting from

telemedicine schemes. And in July 2023, NextGen Healthcare Inc (NextGen), an EHR technology vendor, agreed to pay US$31 million to resolve allegations that NextGen violated the FCA by misrepresenting the capabilities of certain versions of its EHR software and providing unlawful remuneration to its users to induce them to recommend NextGen's software.

Law stated - 16 February 2024

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

11 | What constitutes 'health data'? Is there a definition of 'anonymised' health data?

'Health information' is defined in the principal federal rules that protect patient privacy (the regulations implementing the Health Insurance Portability and Accountability Act (HIPAA) as: 'any information, including genetic information, whether oral or recorded in any form or medium, that . . . "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual' (subject to certain jurisdictional limits).

Under state laws, there are various definitions, but typically they are very broad; for example, Washington State's My Health My Data Act defines 'consumer health data' as information that 'identifies the consumer's past, present, or future physical or mental health status', which includes, but is not limited to:

- individual health conditions, treatment, diseases or diagnosis;
- social, psychological, behavioural and medical interventions;
- health-related surgeries or procedures;
- use or purchase of prescribed medication;
- bodily functions, vital signs, symptoms, or measurements of [health];
- diagnoses or diagnostic testing, treatment, or medication;
- gender-affirming care information;
- reproductive or sexual health information;
- biometric data;
- genetic data;
- precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;
- data that identifies a consumer seeking healthcare services; or
- any information derived or extrapolated from non-healthy information, including by using algorithms or machine learning, that could identify a consumer with indicators of health status.

The HIPAA regulations do not use the term ‘anonymized’ but rather refer to ‘de-identified’ information, which is health information that: (1) contains none of 18 specific identifiers of an individual (or the individual’s employer or family or household members) or (2) has been determined by a qualified expert to present, either alone or in combination with other ’reasonably available information’, no more than a ‘very small’ risk of being identifiable to an individual.

State laws define ‘de-identified data’ somewhat differently; for example, the Washington State law provides that ‘[d]eidentified data’ means ‘data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer, or a device linked to such consumer’, if the holder of the data ‘(a) takes reasonable measures to ensure that such data cannot be associated with a consumer; (b) publicly commits to process such data only in a de-identified fashion and not attempt to reidentify such data; and
(c) contractually obligates any recipients of such data to [do the same].’

Law stated - 16 February 2024

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

At the federal level, health data that is received or created by healthcare providers (with some exceptions) or health insurers (health plans) is protected under the HIPAA regulations, which generally prohibit such entities (covered entities) and their service providers (business associates) from using or disclosing individually identifiable health information without a written authorisation from the individual to whom the information pertains. Persons conducting research using individually identifiable health information also must obtain consent from the subject of the information to use the information for purposes of the research and to share the information with others.

State laws governing healthcare providers and health insurers contain similar requirements for individual consent. Several states have recently enacted laws applicable to persons not governed by HIPAA, which generally require an individual’s consent to collect, use or share any of the individual’s personal health information.

There are no federal laws as protective as HIPAA that apply to other types of personal data, with the exception of certain reputational or financial information, government-issued identification information and children’s information. At the state level, most states that have enacted consumer privacy laws have included in those laws special provisions applicable to ‘sensitive personal information’, which is defined to include personal health information. Under these laws, it is prohibited to use or disclose sensitive personal information without either obtaining the affirmative consent of the individual to whom the information pertains or providing the individual the opportunity to opt out of such use or disclosure.

Law stated - 16 February 2024

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

As noted, the data protection laws in the United States typically refer to de-identified data rather than anonymous data. Health data that has been de-identified is generally subject to prohibitions on *re*-identification by a recipient of the data. Use of de-identified data (data derived from personally identifiable information) is generally not restricted by data privacy laws in the United States, but may be subject to contractual limitations, proprietary claims, etc.

Law stated - 16 February 2024

Enforcement

14 | How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The HIPAA regulations are enforced by HHS' OCR. The Federal Trade Commission (FTC) has broad authority to discipline practices harming consumers, including unfair or deceptive practices involving personal information, and has used that authority in numerous cases involving consumer health information. State data protection laws are generally enforced by the state attorneys general; in some states, such as California, other agencies have been created to enforce these laws. A few, but not many, state laws grant state residents the right to bring a private action to address a claimed violation of state data protection law.

There have been notable enforcement actions. For example, in 2023, the FTC brought suits against two digital health providers, GoodRx and Easy Healthcare, the developer of the fertility app Premom, asserting that the companies intentionally shared users' health data without user authorisation. The FTC also entered a $7.8M settlement with BetterHelp over allegations that the digital mental health platform engaged in unfair and deceptive practices by sharing patient data – in the form of hashed email addresses – with advertisers in a manner that contradicted representations made in the company's privacy policy.

Law stated - 16 February 2024

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

The HIPAA security regulations, 45 C.F.R. Parts 160 & 164, Subpart C, set forth very helpful cybersecurity standards for any entity, regardless of status under HIPAA, that processes personal health information.

The standards published by the National Institute of Standards and Technology (NIST) are highly regarded as exemplary for cybersecurity, and NIST has established a Cybersecurity Framework that may be particularly helpful for digital health offerings.

For digital health offerings that are regulated as medical devices, the FDA has published a variety of guidance and other resources to guide manufacturers on cybersecurity best practices. See Cybersecurity | FDA.

Law stated - 16 February 2024

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

All data of value should be protected by state-of-the-art cybersecurity practices and controls. Personally identifiable health data, including the output of digital health solutions, should be protected not only by strict cybersecurity controls, but also collected, used and shared in a manner that protects the privacy of the individual to whom the data pertains and is consistent with such individual's expectations. Regardless of the requirements and restrictions of applicable law, health information that is identifiable to an individual should be:

- Collected, used and disclosed in a manner that is transparent to the individual – through notice before or at the time of collection.
- Made accessible to the individual upon request, with the exception of information collected as part of a clinical study where the integrity of the study depends on the blinded nature of the study data.
- Used only for purposes described to the individual upon collection or as authorised by the individual thereafter.
- Anonymised prior to use for purposes to which the individual has not consented it be used (ie, before undertaking secondary use).
- Deleted or anonymised when no longer needed.
- Understood to be 'health data' when the information has some connection to an individual's health status or likely health status (such as an IP address collected when an individual explores a website describing mobile health applications).
- Understood to be 'individually identifiable' when it can be traceable to a particular individual's activity, including online.

Law stated - 16 February 2024

INTELLECTUAL PROPERTY

Patentability and inventorship

I

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Key considerations in patenting digital health inventions include subject matter eligibility under 35 USC section 101, inventorship determination and computer-implemented functional claiming under 35 USC section 112. As a threshold patentability requirement, all claimed inventions must be directed to patent eligible subject matter. Typical claims to digital health inventions recite computer-implemented algorithms – which may be considered 'abstract ideas' – a judicial exception to patent eligibility. Nonetheless, applications of abstract ideas may be patentable (1) if the abstract idea is integrated into a practical application, or (2) if the claim as a whole amounts to an inventive concept.

As of the beginning of 2024, method-of-diagnostic claims remain patent-ineligible. The Federal Circuit has also held that claims to an electronic medical records data computing system were patent ineligible because the claims merely recited a well-known abstract process relating to organising healthcare-related information. On the other hand, the Federal Circuit has held that claims to methods of connecting wearable devices to mobile devices were patent eligible because the claims involved inventive ways of arranging devices and using certain protocols.

The case law in this area is evolving. To reduce the uncertainty around patent eligibility, the US Patent and Trademark Office (USPTO) publishes a Subject Matter Eligibility Guidance to improve the clarity, consistency and predictability of examination outcomes. While helpful for navigating the examination process, the Federal Circuit has stated that such guidance is not binding on US courts.

Patents must also name the correct inventors. Inventorship is a legal determination made based on facts. When an invention involves the use of artificial intelligence (AI), the Federal Circuit has held that only a natural person can be an inventor, such that AI cannot be listed as an inventor of a patent application.

On 13 February 2024, the USPTO published an Inventorship Guidance on AI-Assisted Inventions. The guidance sets forth that each inventor named in the patent applications and patents for AI assisted invention must make a 'significant contribution' to the conception of the invention. Furthermore, each claim in an application or patent must have been invented by at least one named inventor, who must be a natural person. The USPTO continues to presume that the inventors named are the actual inventor or joint inventors of the application.

Finally, claims protecting digital health inventions often involve functional claiming language in apparatus claims. For example, a claim may recite certain algorithms implemented on a device, but without naming specific structural elements. The lack of specific structural elements may lead to written description, enablement, or definiteness rejections under 35 USC section 112. The Examiner may also construe the claim as a means-plus-function claim. The USPTO issued Guidance on Examining Computer Implemented Functional Claim Limitations to provide transparency to the public.

Law stated - 16 February 2024

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

Patents for digital health technologies are obtained by filing an application with the USPTO. When all requirements of patentability are met, the application will be granted as a patent. Utility patent applications may be filed to protect the functional aspects of an invention, whereas design patents may be filed to protect the ornamental appearance of an article or product.

To obtain a utility patent, an invention must be directed to patent-eligible subject matter. It must also be useful, novel and non-obvious (35 USC sections 101, 102 and 103). The patent application must include a sufficient written description of the claims to show that the inventor is in possession of the invention, and disclosure enabling a person of ordinary skill in the art to make and use the invention (35 USC section 112).

To obtain a design patent, the invention must be a new, original, ornamental design for an article of manufacture (35 USC section 171). The claimed design must be represented in drawings in compliance with USPTO requirements. The claimed design must be novel, non-obvious, enabled and definite. Because design patents do not protect functional aspects of products, they are useful in protecting instead the ornamental design of products and graphical user interfaces.

Law stated - 16 February 2024

Other IP rights

19 Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

In addition to patents, aspects of digital health offerings may be protected by copyrights, trademarks and trade secrets.

Copyrights protect original works of authorship fixed in a tangible form of expression (17 USC section 102). There is no requirement for registration for the protection to attach, but registration is required to sue under copyright law. Copyrights may be registered at the US Copyright Office. While copyrights do not protect facts, ideas or methods of operation, they are useful in protecting source code and interface designs.

Trademarks identify the source of goods or services in commerce. Common law trademark rights are acquired when a trademark is used in commerce. If desired, trademarks may also be registered at the USPTO or at the state level. To be eligible for federal trademark protection, a trademark must identify and distinguish the relevant goods or services. A trademark may be in the form of a name, word, phase, symbol, image, colour, design or a combination thereof. When properly maintained, trademark protection may last in perpetuity.

Finally, trade secret protections apply broadly to protect business, financial and technical information that meets certain criteria. While patents, copyrights and trademarks require

full disclosure, trade secrets depend on non disclosure. Trade secrets are not registered and may last in perpetuity if preserved properly.

Law stated - 16 February 2024

Licensing

20 What practical considerations are relevant when licensing IP rights in digital health technologies?

IP licensing in the digital health landscape is rather unique, with innovative, early-stage companies developing unique solutions and established, well-funded but less-nimble healthcare, pharma and insurance parties seeking partnerships. As a result, negotiation strength and strategy can take an unexpected turn, with young solution developers having outsized power when compared to traditional licensing relationships. While the value of money and user-base brought by the more traditional, larger player should not be undervalued, smaller digital health technology companies can find themselves coming to the bargaining table with added strength. That said, and while this reality may alter negotiation strategy on both sides, it is not the only practical consideration in digital health transactions in 2024. Consider modern issues around ownership, confidentiality and termination as well.

Intellectual property ownership between two parties who bring very different, but equally impactful elements to the table, can be a challenging consideration with both parties believing they deserve ownership and seek to protect their contributions to a business relationship.

Contemplate the pitfalls of co-ownership of IP as a structure (for varying legal, enforcement and business issues) and instead consider if one-party ownership with a licence back to the other party (limited or broad, when appropriate) is beneficial to the client and relationship. Consider who is funding development, bringing resources (such as users, money, data and support), and supplying a crucial technology base when advising on ownership of developed IP.

Further, consider how data sets should be handled from ownership, use and confidentiality standpoints - Which party is getting access to data sets (and other IP) of the other party, how can it be used and how should it be held by the receiving party as confidential? Regarding use, remember to consider how the parties should be entitled to use these data sets both for traditional uses (marketing, benchmarking, etc) and modern uses (training of AI and similar algorithms using both the data inputs of either or both parties and the exported data, whether in its entirety or in aggregate).

Finally, consider how can rights be deployed during the term of the relationship and how long (if at all) they should survive, and in what form, following expiration or termination of the relationship?

Law stated - 16 February 2024

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

With many of the innovative developments in digital health coming from younger and not always fully funded startups, securing mechanisms for enforcing IP rights and protecting partnership investments in such companies is more crucial than ever for established partners. Beyond traditional and contractual enforcement mechanisms, companies seeking to partner with digital health players (particularly earlier-stage ones) may consider alternate strategies including software or tech escrow protections, rights of first refusal on future inventions and warrants, or other investment opportunities to protect partnership investments

With respect to recent patents-related enforcement, while patents are presumed valid once issued, courts may dismiss cases involving digital health patents upon finding that a patentee has failed to state a claim because the asserted patents are invalid under 35 USC section 101. Patentees may wish to pre-emptively include factual allegations supporting the asserted patents' validity in the complaint. The Federal Circuit has held that patent claims to computer-implemented methods were directed to an abstract idea, but the methods 'plausibly' recite a specific implementation to solve a problem to overcome a motion to dismiss. The District Court of Delaware also recently denied a motion to dismiss based on finding that asserted claims to a user interface were not directed to unpatentable subject matter.

Law stated - 16 February 2024

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

The advertising-related laws that apply can differ depending on the type of digital health product and its regulatory status. For digital health products subject to Food and Drug Administration (FDA) oversight as medical devices, promotional labelling and marketing claims must be consistent with the intended use cleared or approved in the underlying marketing authorisation (PMA, 510(k), or *de novo* authorisation). For devices that are exempt from the marketing authorisation requirements (generally low-risk, Class I devices), labelling and marketing claims must be consistent with the scope of the exempt classification. In all cases, labelling and marketing claims for digital health devices must be truthful and non-misleading and appropriately substantiated. The type of substantiation necessary to support a claim depends on the nature of the claim and the regulatory status of the underlying product.

For digital health devices, while the FDA has primary jurisdiction over labelling, the FDA and Federal Trade Commission (FTC) have shared jurisdiction over advertising (with the FDA having primary authority over 'restricted' devices). Both agencies can take action

against false or misleading advertising of medical devices and sometimes coordinate on enforcement efforts. The FTC's statutory authority stems from the FTC Act, which prohibits unfair or deceptive advertising. In December 2022, the FTC issued an updated Health Products Compliance Guide, with recommendations on how to ensure that claims about the benefits and safety of health-related products – including specifically health-related apps – are truthful, not misleading, and supported by science. The FTC's oversight applies to the advertising of both device and non-device digital health technologies.

In addition, many states have similar consumer protection or deceptive advertising-related laws.

Law stated - 16 February 2024

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

E-commerce laws govern many different areas that can affect digital health offerings. To give just a few examples, this can include laws relating to health breach notifications, informed consent and disclosures, privacy policies, electronic signatures, use of texts and telemarketing, advertising, copyright and intellectual property, as well as various other consumer protection laws at both the federal and state level.

Law stated - 16 February 2024

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Yes, digital health products and services are covered and reimbursed by federal programs like Medicare and Medicaid, but coverage and reimbursement may vary based on the type of product or service. 'Digital health' is a broad term that refers to a blend of technology and healthcare, and encompasses many types of tools and services, such as cell phone applications, devices (eg, heart monitors), digital therapeutics (eg, software programs for care management or treatment) and telehealth. Both the Medicare and Medicaid programs cover and pay for telehealth services depending on the particular service and under certain conditions. Certain telehealth flexibilities (eg, temporary removal of geographic and site requirements) afforded during the covid-19 pandemic and public health emergency remain in place under Medicare through 2024. Medicare also covers services such as remote patient monitoring and remote therapeutic monitoring. There have been limitations on coverage and reimbursement of digital therapeutics, however, given the structure of the Medicare programme and scope of benefit categories.

Law stated - 16 February 2024

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

In 2023, there were significant developments in many different facets affecting the digital health sector. To highlight one notable area, with the broader adoption of use of AI in digital health services and technologies, regulators continued to grapple with how best to regulate AI in healthcare in a manner that balances fostering innovation with protection of patient and consumer safety. To that end, on 30 October 2023, President Biden signed an executive order that directs the Department of Health and Human Services to create an AI Task Force charged with developing a strategic plan on the responsible deployment and use of AI-enabled technologies in the healthcare sector. The plan would include policies and frameworks, as well as regulatory action where appropriate. Areas to be addressed in the plan include development and use of predictive and generative AI-enabled technologies in healthcare delivery and financing, long-term safety and real-world performance monitoring of AI-enabled technologies, incorporation of equity principles in AI-enabled technologies, and incorporation of privacy and security standards into the software development life cycle for protection of personally identifiable information.

The authors gratefully acknowledge the assistance of Josh Blankand Angela Vicari in writing this chapter.

Law stated - 16 February 2024

Abeba Habtemariam abeba.habtemariam@aporter.com
Nancy L Perkins nancy.perkins@aporter.com
Chris Anderson christopher.anderson@arnoldporter.com
Monique Nolan monique.nolan@arnoldporter.com
Alice Ho alice.ho@arnoldporter.com

Arnold & Porter