DIGITAL HEALTH

China

LEXOLOGY
Getting The Deal Through

Digital Health

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 25 January 2022

Table of contents

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

Investment climate

Recent deals

Due diligence

Financing and government support

LEGAL AND REGULATORY FRAMEWORK

Legislation

Regulatory and enforcement bodies

Licensing and authorisation

Soft law and guidance

Liability regimes

DATA PROTECTION AND MANAGEMENT

Definition of `health data'

Data protection law

Anonymised health data

Enforcement

Cybersecurity

Best practices and practical tips

INTELLECTUAL PROPERTY

Patentability and inventorship

Patent prosecution

Other IP rights

Licensing

Enforcement

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

e-Commerce

PAYMENT AND REIMBURSEMENT

Coverage

UPDATES AND TRENDS

Recent developments

Contributors

China

David Chen
David.Chen@ropesgray.com
Ropes & Gray LLP

Katherine Wang
Katherine.Wang@ropesgray.com
Ropes & Gray LLP

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

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

Key players include:

- central Chinese government and sectoral regulators;
- private healthcare businesses, including entrepreneurs and start-up businesses, which are concentrated along the Yangtze River Economic Belt, the Greater Bay Area and the Beijing/Tianjin Area;
- insurance companies;
- healthcare professionals;
- venture capital and private equity funds; and
- academic institutions.

Key areas of innovation include internet hospitals, including telehealth and virtual health services, online pharmacy, AI-assisted patient diagnosis and patient screening, big data, and e-referral and booking capabilities. Internet hospitals are developing rapidly, driven by favourable government policy and the ongoing covid-19 pandemic. As a result, internet diagnosis and treatment and online drug purchasing have become increasingly habitual in China. Users for online consultation, medical e-commerce, health management and other platforms have also experienced significant growth over the last year.

Law stated - 30 November 2021

Investment climate

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

Digital health technologies have become a trendy investment focus of investors in the healthcare industry in China as Chinese increase their adoption of digital health technologies. The covid-19 pandemic catalysed accelerated investment in digital health and facilitated greater coordination between private and public sector participants. The healthcare space in China is in general highly regulated and shifting government policies add a layer of uncertainty to the overall investment climate.

Law stated - 30 November 2021

Recent deals

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

Some notable recent deals in the digital health sector in China include:

- October 2021: Tencent backed Yuanxin Tech, the operator of Miaoshou Doctor, an online medical platform, filed for an IPO on Hong Kong Stock Exchange (HKEX). Previously, Yuanxin Tech had completed a series F round raising over 1.5 billion yuan from investors including Sequoia Capital China.
- September 2021: On 7 September, ByteDance invested 200 million yuan to invest in the mental health internet

medical platform, Haoxinqing, the largest domestic investment in the mental health field to date. Also, on 9 September, ByteDance's medical brand, Xiaohe Yiliao, invested an undisclosed amount in two medical companies founded by Hu Lan, Amcare Healthcare (Meizhong Yihe) and Hongda Airui, taking 17.57 per cent and 10.71 per cent ownership, respectively.

- August 2021: Zhiyun Health, China's largest provider of digital chronic disease management solutions, filed for an IPO on HKEX. Previously, Zhiyun Health had received several rounds of financings from domestic and foreign investors, including SIG, IDG, CICC Capital, and China Merchants Bank International.
- April 2021: Tencent-backed digital health platform, WeDoctor, filed for its long-awaited IPO on HKEX. WeDoctor is valued close to US$7 billion.

Law stated - 30 November 2021

Due diligence

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

Key due diligence issues to understand and resolve include:

- IP/Technology: ensuring that the digital health venture has sufficient ownership or rights to use the data, software, intellectual property, and technology that is key to its business. Attention should also be paid to the enforceability of the digital health venture's intellectual property.
- Data: understanding the types of data collected and held by the digital health venture, how such data is obtained and used, cross-border and third party transfers of such data, the importance of such data to its business and its competitive advantage, and compliance with the relevant data protection regulations. In particular, if it collects human genetic resources data and transports such data to a foreign entity, it is important to review its compliance with China's regulations on human genetic resources.
- Exclusivity: understanding the digital health venture's exclusive rights to its technology and intellectual property, and any non-compete and other exclusivity covenants that may constrain a digital health venture's business or growth.

- Regulatory: verifying that the digital health venture has obtained all necessary permits and licences relevant to its products and services, or has a viable pathway to obtain them.
- Privacy: ascertaining whether the digital health venture's processing of personal information of Chinese individuals is compliant with applicable data privacy laws, including review of the lawful collection or acquisition of personal information, the legal bases for processing it, privacy notices, privacy consents, cross-border and third-party transfers, and data security practices.
- Cybersecurity: understanding the digital health venture's information security practices, including whether or not it has experienced any information security or cybersecurity incidents, been the subject of regulatory investigations or complaints relating to its cybersecurity practices.

Law stated - 30 November 2021

Financing and government support

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 and private equity funding are common sources of financing in the digital health sector and the Variable Interest Entity (VIE) structure is commonly adopted. Historically, the VIE structure came about as a 'workaround' to allow indirect investment in industries in China in which foreign investment was restricted or prohibited by the government, such as media and telecommunications. A typical VIE structure involves a Cayman company at the top, a Hong Kong intermediary at the middle and a Wholly Foreign-Owned Enterprise (WFOE) at the bottom. The WFOE usually exercises de facto control over the operations and management of a domestic PRC entity which holds the necessary permit or permits to operate in a sector in which foreign investment is restricted or prohibited. Public financing through IPOs is also on the rise. A significant number of digital health companies filed for their IPOs in 2021.

Amid the peak of covid-19 in March 2020, the Chinese government issued clear guidance supporting reimbursement of internet healthcare. The implementation of national health insurance (NHI) policy is conducive to building a stable and sustainable profit model for digital health ventures. Four months later, the State Council released a set of key tasks for the medical system, which included incorporating big data, video monitoring, facial recognition, and other new generation information technologies.

Law stated - 30 November 2021

LEGAL AND REGULATORY FRAMEWORK

Legislation

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

China does not have an omnibus statute governing the digital health sector. Different laws, regulations and guidelines apply depending on business and its products or services.

A digital health product that falls under the definition of a medical device under the Regulations on the Supervision and Administration of Medical Devices (Revised in 2021) (Order #739) is regulated as a medical device. The R&D, manufacturing, distribution and use of medical devices in China are governed by Order #739.

The provision of medical services by hospitals and health care professionals is governed by the Law of the People's Republic of China on Basic Medical and Health Care and the Promotion of Health . Various administrative rules governing the provision of medical services via digital means also generally apply to the digital health sector, including the Measures for the Administration of Internet Diagnosis and Treatment (for Trial Implementation) , the Measures for the Administration of Internet Hospitals (for Trial Implementation), and the Specifications for the Administration of Remote Medical Services (for Trial Implementation).

The advertising and promotion of digital health products and services are primarily governed by the Advertising Law (revised in 2021) , the Interim Administrative Measures for the Review of Advertisements for Drugs, Medical Devices, Dietary Supplements and Food for Special Medical Purposes , and the Measures for the Administration of Medical Advertisements . Restrictions on marketing practices are set out in the Anti-Monopoly Law , the Anti-Unfair Competition Law , and their related regulations.

Since the digital health sector is highly dependent on the processing of personal information, and may involve the processing of important data, which are subject to stricter regulation, China's data security and privacy laws are of great importance. The Personal Information Protection Law (PIPL) , the Cybersecurity Law, the Data Security Law

(DSL), and Biosecurity Law constitute the four pillars of China's data security and privacy governance regime applicable to the digital health sector. Additionally, the National Health and Medical Big Data Standards, Security and Service Management Measures (Trial) applies digital health companies engaging in medical data big data.

The collection, handling and export of data derived from human genetic resources (HGR) is subject to the Biosecurity Law and the Regulation on the Administration of Human Genetic Resources . These laws and regulations formalise a longstanding practice requiring that foreign-owned entities seeking access to China's HGRs can only do so through collaborations with Chinese partners.

Furthermore, as the digital health products and services often utilise or are deployed via websites, mobile APPs, or other online platforms, China's regulations on mobile APPs, e-commerce, and online platforms generally apply, including the Telecommunications Regulations , the E-Commerce Law , the Administrative Provisions on Mobile Internet Applications Information Services and the Announcement of App Security Certification Work .

Law stated - 30 November 2021

Regulatory and enforcement bodies

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

Various regulatory and enforcement bodies in China have jurisdiction over the digital health sector.

- The National Medical Product Administration (NMPA), under the State Administration for Market Regulation (SAMR), is the primary regulator of digital health products in China. It is tasked with granting marketing authorisations and carrying out post-approval supervision.
- At the national level, the National Health Commission (NHC), the health department under the State Council, regulates the operation of public hospitals and health care professionals.
- The SAMR regulates the advertising and promotion of digital health products.
- The National Healthcare Security Administration (NHSA) regulates centralised procurement and reimbursement of digital health products under the Chinese Basic Medical Insurance (BMI) scheme.
- The Cyberspace Administration of China (CAC) and the Ministry of Public Security (MPS) are tasked with formulating data security and privacy laws and regulations and ensuring their compliance within the scope of their respective functions.
- At the provincial, municipal and county level, local counterparts of the NMPA, SAMR, NHC, NHSA, CAC, and MPS have rulemaking and enforcement authority over their regions, subject to national laws and regulations defining the scope of their administrative authority.
- The Human Genetic Resources Administration of China (HGRAC), an administrative entity under the Ministry of Science and Technology, is the primary regulator of the collection, handling and export of China human genetic resources (HGR) and data derived from HGR.
- The Ministry of Industry and Information Technology (MIIT) and local Communications Administrations also have an important role in regulating the digital health sector. They are in charge of formulating and implementing rules governing internet content provider (ICP) licensing and record filing, which apply to digital health products and services that provide information services via the internet.

Law stated - 30 November 2021

Licensing and authorisation

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

Digital health products, such as healthcare apps, wearables and Software as a Medical Device (SaMD), that fall under the definition of a medical device under the Medical Device Regulation (Order #739) are regulated as medical devices. Medical devices in China are classified into three categories based on the product's risk profile. All medical devices in China must be approved in prior to marketing. Class I medical devices are subject to recordation filing requirements. Class II and Class III medical devices are subject to product registration requirements. Accordingly, digital medical devices that are classified as Class II or Class III medical devices need to be registered with the NMPA or its provincial counterparts as medical devices. Clinical trial authorisation from the NMPA is required for Class III medical devices with a higher risk profile before conducting clinical trials involving such devices.

Additional requirements may apply to the provision of digital health services, especially with respect to the provision of medical services by medical and healthcare institutions. Medical institutions are required to obtain practicing licences. Medical and healthcare institutions of all types and at all levels are also required to comply with regulations for medical and healthcare institutions issued by the Ministry of Health and its local counterparts. China has a medical practice registration system for doctors, nurses and other medical and healthcare professionals.

Distributors of drugs or medical device products via the internet need to obtain a distribution permit from local Medical Product Administrations (MPAs) if they are not the marketing authorisation holders for the products. Platform enterprises who provide online transaction-related services related to healthcare need to obtain an internet pharmaceutical information services licence from local MPAs and obtain an ICP filing or licence from local Communications Administrations.

Law stated - 30 November 2021

Soft law and guidance

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

There are a number of government and regulatory policy documents and technical standards that constitute 'soft' law or guidance governing digital health, including:

- Guiding document issued by the central Chinese government and sectoral regulators: the Guiding Opinions of the State Council on Actively Propelling the Internet Plus Action Plan and ' are some of the policy documents that have been published outlining the central government's advocacy for the development of the digital health sector. The Guiding Opinions of the National Healthcare Security Administration on Actively Promoting Medical Insurance Payment for 'Internet Plus' Medical Services outlines the Chinese government's views on implementing uniform medical insurance payment system for online and offline medical services.
- Technical Review Guidance from the NMPA: various guiding principles issued by the NMPA, such as the Guiding Principles for the Technical Review of Medical Device Software Registration, the Guiding Principles for the Technical Review of Mobile Medical Device Registration, and the Guiding Principles for the Technical Review of the Cybersecurity Registration of Medical Devices, specify the legal requirements for the registration of medical devices.

- Cybersecurity and data privacy: various non-binding national standards are key instruments for implementing China's cybersecurity and data protection and privacy laws. These include, for data privacy, the Information Security Technology: Personal Information Security Specification (2020) (PIS Specification), for network security, various national network security standards, including GB/T 22239-2019 Information security technology — Baseline for classified protection of cybersecurity, GB/T 25070-2019 Information security technology — Technical requirements of security design for classified protection of cybersecurity, GB/T 25058-2019 Information security technology — Implementation guide for classified protection of cybersecurity, and GB/T 28449-2018 Information security technology — Testing and evaluation process guide for classified protection of cybersecurity.

Law stated - 30 November 2021

Liability regimes

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 improper provision of digital health products and services in China can result in administrative, civil or criminal liabilities. Manufacturers and distributors of a defective digital health product or service may also be subject to tort liability and bear joint and several liability for death, injury, or other damages of consumers caused by the defective product or service. Medical institutions that use defective digital health products or services on patients can also be held liable but have a statutory right of recourse against the responsible marketing authorisation holders or manufacturers of the defective product or service. It is common in China for businesses to purchase liability insurance to cover product liability claims.

Digital health products and services providers bear administrative liabilities and penalties if they violation applicable laws and regulations. For example, liabilities and penalties under Order #739 include revocation of administrative approval, forfeiture of illegal proceeds, confiscation of illegal products, tools, equipment or raw materials, administrative fines of up to 30 times the illegal income, debarment from future regulatory applications for up to 10 years, and suspension of business operations (in serious cases). Responsible individuals may also be subject to personal liability for non-compliance in serious cases. Corporate and personal liability are also possible if the processing of personal information by digital health products or services violates the applicable data privacy laws. For example, a digital health products or services provider that violates the PIPL may be subject to significant penalties for serious violations, including rectification orders, confiscation of illegal gains, business suspension, revocation of business licences, and, most notably, fines of up to 50 million yuan or 5 per cent of turnover in the previous year.

Furthermore, failure to fulfil certain statutory obligations, such as data security and data privacy obligations, may also result in criminal liabilities. For example, illegally selling or providing Chinese citizens' personal information to others may constitute a crime under the PRC Criminal Law and result in fines and up to seven years imprisonment in serious cases.

Many laws and regulations applicable to the digital health sector have an extra-territorial reach, and therefore the liability regimes as explained above are generally applicable to the cross-border provision of digital health products and services.

Law stated - 30 November 2021

DATA PROTECTION AND MANAGEMENT

Definition of `health data'

What constitutes ‘health data’? Is there a definition of ‘anonymised’ health data?

There is no uniform definition of ‘health data’ under Chinese law. Different laws and regulations have different definitions that apply to their jurisdictional scope. However, in general, the following categories of data are generally considered to be ‘health data’ in China: (1) human genetic resources data, regulated under the Biosecurity Law and the Regulations on the Administration of Human Genetic Resources , (2) medical records or medical device data, regulated under the Regulations for Medical Institutions on Medical Records Management , and (3) population health information, regulated under the Population Health Information Management Measures (Trial Implementation) .

Law stated - 30 November 2021

Data protection law

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, genetic data, and biometric data are considered sensitive personal information under the PIPL. Sensitive personal information is generally afforded a higher level of protection than ordinary personal information. Processing of sensitive personal information requires the personal information processor to ensure:

- data subjects have given their explicit, separate consent;
- data subjects have been notified of the purposes, necessity, methods, scope, duration of storage, and impact on an individual’s rights and interests of the processing;
- strict protection measures, including encryption, role- and need-based access control mechanisms, are implemented;
- for the processing of personal information of minors under the age of 14, consent of the parent or other guardian of the minor is obtained, and that specialised rules for the processing of such personal information are formulated;
- a privacy impact assessment is performed in advance of such processing;
- before sharing, transferring or publicly disclosing sensitive personal information, data subjects are informed of the types of sensitive personal information involved, the identity of the recipient and their data security capabilities, and provide explicit consent in advance; and
- data subjects are promptly notified of any security breach involving their sensitive personal information.

Law stated - 30 November 2021

Anonymised health data

Is anonymised health data subject to specific regulations or guidelines?

Under the PIPL, ‘anonymised’ data refers to personal information that has been processed so that the identification of specific individuals is impossible and unrecoverable. Anonymised data is no longer considered personal information under Chinese data protection and privacy laws, and is generally regulated the same as ordinary data. It is worth noting, however, that even anonymised data may still be considered as ‘important data’ or ‘medical big data’ and be subject to stricter control over storage and outbound transmission.

Law stated - 30 November 2021

Enforcement

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?

Numerous regulators have overlapping jurisdiction when it comes to enforcing data protection laws in China. Some of the key regulators include CAC, MPS, SAMR, and MIIT.

Since the data protection and privacy laws in China are still relatively new, there have not been very many notable enforcement actions in the digital health sector.

Law stated - 30 November 2021

Cybersecurity

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

The Cybersecurity Law is the primary data security and privacy legislation regulating network operators in China, including digital health products and service providers that operate or manage networks. China has implemented a network security framework known as the 'Multi-Level Protection Scheme' (MLPS) as part of the Cybersecurity Law, under which network operators are required to take appropriate cybersecurity measures corresponding to the classification of their information system (ranging from level 1 to level 5). The latest framework is commonly known as MLPS 2.0. Digital health businesses need to take steps to comply with MLPS 2.0, taking reference of the relevant standards that have been published.

In addition, for digital health businesses, data security incidents involving the theft of personal information is a major risk. Although not mandatory, the PIS Standard is a key guideline for compliance and is widely adopted by Chinese companies. Some of its key principles and requirements that are of particular relevance to digital health businesses include:

- Minimisation principle: the PIS Standard requires businesses to only process types and quantities of personal information necessary for the purposes for which the authorised consent is obtained, and to delete all personal information promptly after the purpose for the processing is achieved.
- Processing of sensitive personal information: the PIS Standard recommends that prior to collecting sensitive personal information (which includes any medical data, genetic data, or biometric information), businesses need to inform data subjects of the necessity of such collection, the consequence of not consenting to the collection and providing such information, and the associated risks in case of data breach. The PIS Standard also requires businesses processing personal sensitive information to conduct a personal information security impact assessment to evaluate the risks that their processing activities could harm the lawful rights and interests of data subjects and how effective their security measures are in mitigating such risks.

Cyber insurance coverage is recommended and is increasing in importance as China's data protection and privacy

regime becomes mature, and the possibility of increased penalties, fines, and liability for cyber breaches increases. Appropriate coverage limits will vary depending on the number of users of the products and services of a digital health business, the type of personal information that is collected and processed, and the size of the digital health business.

Law stated - 30 November 2021

Best practices and practical tips

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 businesses should bear in mind the minimisation principle discussed above and take a proactive approach to data protection and privacy compliance. Good data protection and privacy practices can only be achieved through a comprehensive, company-wide approach and sustained effort.

In practice, the minimisation principle means that digital health businesses should make conscious decisions concerning what and how much personal information they actually need to collect for their business functions, and whether they actually need to transfer or share personal information to China and non-China affiliates, to third parties, or outside of China.

Lastly, digital health businesses may need to comply with data localisation requirements if they are considered critical information infrastructure operators or when they process personal information beyond a government-prescribed threshold amount. When there is indeed a need to transfer any personal information outside of China, digital health businesses need to meet certain statutory requirements for outbound transfer.

Law stated - 30 November 2021

INTELLECTUAL PROPERTY

Patentability and inventorship

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

Except for certain non-patentable subject matter (for example, rules and methods of intellectual activities, genetic sequences, methods of diagnosing or treating diseases, or animal or plant varieties), in general, inventions that meet the patentability requirements can be claimed in a patent. Both method claims and product claims can be claimed for digital health-related inventions.

Digital health-related inventions (such as software, algorithms, business rules, databases and AI-generated content) that only claim rules and methods for intellectual activities are not patentable. However, such inventions can be patented if they also include technical features (that is, the invention uses technical means to solve technical problems and obtain technical effects).

Law stated - 30 November 2021

Patent prosecution

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

Digital health technologies may be eligible for patent protection in China as a patentable invention (method or device), utility model (device only), or design (device only). Under the PRC Patent Law, the term and examination procedure for these three kinds of patents are as follows:

- invention patent: term is 20 years from the filing date, and procedure requires both preliminary examination and substantive examination;
- utility patent: term is 10 years from the filing date, and procedure requires preliminary examination; and
- design patent: term is 15 years from the filing date, and procedure requires preliminary examination.

The patent application and registration procedure for patentable digital health technologies is generally the same as for other patentable inventions, utility models, and designs. To file a patent application, the owner of the invention or the right to file a patent for the invention needs to engage a PRC patent agent. A patent application, disclosing the invention in a clear and complete manner, must be prepared and submitted to the China National Intellectual Property Administration (CNIPA), and official filings fees must be paid. For an invention patent application, a substantive examination of the patentability of the patent must be conducted by CNIPA.

Law stated - 30 November 2021

Other IP rights

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

Data, algorithms, and software are important categories of intellectual property for digital health technologies. In China, software, and to some extent, databases, are protected by copyright. By default, the copyright is owned by the author or company that generates or develops such software or database.

Proprietary know-how that has commercial value are protectable in China as trade secrets. Consequently, trade secrets are another means of protecting digital health technologies that are not suitable for other forms of IP protection.

Law stated - 30 November 2021

Licensing

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

Some key practical considerations for IP licensing transactions involving digital health technologies include:

- Data rights and ownership: it is important to understand, as between the licensor and licensee, who owns the data generated under the licence agreement, how such data will be used, whether such data will be shared between the parties, who owns the insights or technology derived from the use of such data, and whether revenue resulting from the use of such data or technology will be shared.

- Scope of IP being licensed and rights of access: it is important to clearly define what IP is being licensed, whether it includes all the IP that is needed for a party to exploit the technology, and whether it contains updates or new IP that is later created. For software licences, it is important to clearly define the versions and features of the software being licensed, and whether updates are included.
- Exclusivity v non-exclusivity: it is important to understand which licensed rights are granted on an exclusive basis and which are granted on a non-exclusive basis, as it will impact what a licensee can do with the IP rights obtained and what a licensor can do with the IP rights that are licensed.
- Termination provision: triggers for termination and the effects of termination are usually heavily negotiated provisions in a licence agreement, particularly if licensed rights are granted exclusively.
- Performance targets: the parties often need to determine what are their respective obligations for utilising the licensed IP, and what are the consequences if a party's performance falls short of expectations.
- Regulatory obligations: the parties should ensure to comply with any export control, HGRAC regulations and other data related regulations and may want to set out specific compliance provisions in the agreement.

Law stated - 30 November 2021

Enforcement

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?

Civil litigation and administrative enforcement actions are the two most relevant options for enforcing IP rights in digital health technologies.

Civil litigations typically occur with the following steps:

- The enforcing party investigates and gathers evidence of infringement.
- The enforcing party files applications for preliminary relief, evidence preservation and property preservation with the People's Court, followed by a formal civil complaint and supporting evidence. The defendant can submit a formal defence and rebuttal evidence. For enforcement of patents, the defendant can file a patent invalidation application with the Patent Re-Examination Board at any time.
- An oral hearing is conducted and decision is rendered by the People's Court.
- Either party can appeal the decision by filing an appeal with the higher-level People's Court.

Administrative enforcement actions typically occur with the following steps:

- The enforcing party investigates and gathers evidence of infringement.
- The enforcing party files an administrative complaint with the CNIPA or its local office or other administrative authority.
- The relevant administrative authority investigates and takes action to obtain evidence of infringement. The defendant can submit a formal defence and rebuttal evidence. Oral hearings may be conducted.

- The administrative authority issues a decision.
- Either party can appeal the decision by filing an administrative lawsuit with the People's Court.

Mindray Biomedical Electronics Co, Ltd v Shenzhen Huasheng Medical Technology Co, Ltd is a recent notable case

involving digital health technologies, which was decided in July 2020. In the case, Mindray sued Huasheng to enforce its patent relating to 'Body Map Operation Methods and Systems for Ultrasound Diagnostic Equipment'. The Supreme People's Court ruled in the Mindray's favour and awarded damages of 1 million yuan to compensate Mindray for its economic losses and reasonable enforcement costs.

Law stated - 30 November 2021

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

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

The advertising of digital health products is primarily regulated under the Advertising Law (revised in 2021) and the Interim Administrative Measures for the Review of Advertisements for Drugs, Medical Devices, Dietary Supplements and Food for Special Medical Purposes . The Advertising Law defines advertising activities broadly, covering any channels or media where a distributor of a product or service directly or indirectly markets or introduces the product or service. Where a digital health product is regulated as a medical device, any advertisement of such product requires the prior approval of the local Administration of Market Regulation. In China, common issues with advertisements of medical devices including prohibited off-label advertising, unscientific or misleading statements, guarantees of efficacy or safety, and endorsements by health care professionals, scientific experts, and patients.

The Measures for the Administration of Medical Advertisements regulates the advertising of digital health services. Before publishing a medical advertisement that directly or indirectly introduces medical institutions or medical services, the relevant medical institutions must submit the draft script to and obtain an Examination and Approval Certificate of Medical Advertisements from the local provincial counterpart of the NHC. Medical advertisements can only contain the basic information stated on the medical institution's medical licence, such as the name, address, ownership, type, clinical departments, and number of beds, etc. Medical advertisements cannot contain any reference to medical technologies, diagnostic methods, names of diseases, names of drugs, cure rate guarantees, denouncement of competitors, or the names and images of physicians, patients, or medical education or research organisations. In addition, medical advertisements may not be disguised as news coverage.

Law stated - 30 November 2021

e-Commerce

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

The E-Commerce Law sets out specific requirements for use of electronic payments and conclusion of contracts in e-commerce which apply to the offering and selling of digital health products and services online. Buyers and sellers of digital health products and services through e-commerce may agree to adopt electronic payment methods. For digital health products that are considered medical devices, the Measures for the Supervision and Administration of Online Sales of Medical Devices issued by the NMPA also govern their online sale.

Law stated - 30 November 2021

PAYMENT AND REIMBURSEMENT

Coverage

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

In China, as a precondition for the reimbursement of the costs of a drug through Basic Medical Insurance (BMI), the drug must be listed in the National Drug Catalogue for Basic Medical Insurance (also known as the Reimbursable Drug List, RDL). Similar to drugs, only treatments or devices included in the Catalogue for Medical Treatment Charges Covered by BMI are reimbursable. The reimbursement landscape for medical devices and medical treatments is more fragmented compared to that for drugs. Specific reimbursement ratios and caps for medical devices and medical treatments are set at the discretion of individual cities and vary significantly across the nation.

Digital health products and services that are listed in the RDL and the Catalogue for Medical Treatment Charges Covered by BMI are reimbursable. For example, artificial intelligence assisted treatment technology is reimbursable in Shanghai and the reimbursement rate is 80 per cent.

An increasing number of private health insurers are expanding their insurance coverage to cover digital health products and services.

Law stated - 30 November 2021

UPDATES AND TRENDS

Recent developments

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 significant legislative developments in the past few years affecting the digital health sector in China related to data protection. For the healthcare industry, GB/T 39725-2020 Information security technology – Guide for health data security , a new national standard became effective in July 2021. The guidelines provide recommended methods for classifying and categorising health data, and recommended security measures when processing health data in different scenarios, including clinical research, secondary utilisation, medical devices, connections between commercial insurance and social insurance, and mobile applications.

Law stated - 30 November 2021

Jurisdictions

Australia	Gilbert + Tobin
Brazil	Gusmão & Labrunie
China	Ropes & Gray LLP
Czech Republic	dubanska & co
Germany	Ehlers Ehlers & Partner
India	Chadha & Chadha Intellectual Property Law Firm
Indonesia	ABNR
Ireland	Mason Hayes & Curran LLP
Israel	Naschitz Brandes Amir
Japan	Anderson Mori and Tomotsune
Qatar	Al Marri & El Hage Law Office
Russia	King & Spalding LLP
South Korea	Bae, Kim & Lee LLC
Spain	Baker McKenzie
Switzerland	Lenz & Staehelin
Thailand	Baker McKenzie
United Kingdom	Latham & Watkins LLP
USA	Seyfarth Shaw LLP