International
Comparative
Legal Guides

Practical cross-border insights into digital health law

# Digital Health

# 2023

## Fourth Edition

Contributing Editor:
**Roger Kuan**
**Norton Rose Fulbright**

ICLG.com

# Introductory Chapter



# Expert Analysis Chapters



# Q&A Chapters

# China



Cindy Hu


Jason Gong


Jiaxin Yang

East & Concord Partners


## 1 Digital Health

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

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

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

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

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

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

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

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

Influenced by COVID-19, China's online medical advantages have been highlighted, and the market share of digital health has increased continuously. According to the digital health report "2022 (I) China Digital Health Market Data Report", by June 2022, the market size of China's Internet medical industry has reached CNY 309.9 billion and the transaction size of the pharmaceutical e-commerce industry has reached CNY 239 billion. It is estimated that the scale of China's digital health market will increase to CNY 4,222.8 billion in 2030, with a compound annual growth rate of 30.9%.

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

According to the relevant industry data, as of June 30, 2022, the top five digital health companies are JD Health, Alibaba Health, Ping An HealthKonnect, We Doctor and Miaozhou Doctor.

## 2 Regulatory

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

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

- Law of the PRC on the Promotion of Basic Medical and Health Care.
- Regulation on the Administration of Medical Institutions.
- Administrative Regulations on Application of Electronic Medical Records (for Trial Implementation).
- Administrative Measures on Standards, Security and Services of National Healthcare Big Data (for Trial Implementation).
- Administrative Measures for Internet-based Diagnosis (for Trial Implementation).
- Administrative Measures for Internet Hospitals (for Trial Implementation).
- Administrative Regulations on Telemedicine Services (for Trial Implementation) ("Administrative Regulations on Telemedicine Services").
- Detailed Rules for the Supervision of Internet Diagnosis and Treatment (for Trial Implementation).
- Guiding Opinions of the State Council on Vigorously Advancing the "Internet Plus" Action.

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

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

The other core regulatory schemes include the following:

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

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

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

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

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

The principal regulatory authorities include the following:

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

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

Personal information protection, data security and cybersecurity

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

### 2.6 What regulations apply to software as a medical device and its approval for clinical use?

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

### 2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

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

## 3 Digital Health Technologies

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

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

### 3.2 What are the key issues for digital platform providers?

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

## 4 Data Use

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

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

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

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

If the entity involved is a third party that obtains relevant personal information through sharing or joint processing in accordance with the terms of the relevant agreement, it shall process the personal information in accordance with the relevant agreement and shall not process personal information beyond the agreed processing purpose and method. If it infringes on individuals' rights and interests in terms of personal information and causes damage, it shall bear joint and several liability in accordance with the law.

If the entity involved is located overseas and has one of the following circumstances: 1) providing products or services to domestic natural persons; 2) analysing and evaluating the behaviour of domestic natural persons; or 3) under other circumstances stipulated by laws and administrative regulations, the said entity shall establish a special institution or designated representative within the territory of the PRC to handle matters related to personal information protection, and submit the name of the relevant institution or the name and contact information of the representative to the relevant department responsible for personal information protection.

If the entity involved falls within the definition of the critical information infrastructure operator ("CIIO"), it shall also abide by the Regulations on Security Protection of Critical Information Infrastructure.

### 4.3 Which key regulatory requirements apply?

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

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

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

### 4.4 Do the regulations define the scope of data use?

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

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

### 4.5 What are the key contractual considerations?

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

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

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

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

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

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

### 4.7 How are issues with data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The Technical Guide for Clinical Trial Data Management regulates the management of clinical trial data and the prevention and treatment of data errors and deviations from the following aspects: the responsibilities, qualifications and training of data management-related personnel; the requirements of the management system; the standardisation of test data; the main contents of data management; the guarantee and evaluation of data quality; and safety data and severe adverse drug reaction cases.

## 5 Data Sharing

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

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

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

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

In addition to meeting the general data-sharing requirements, entities of different natures should also comply with other relevant provisions, for example:

If the sharing party is the CIIO, it shall also abide by the Regulations on Security Protection of Critical Information Infrastructure.

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

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

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

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

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

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

## 6 Intellectual Property

### 6.1 What is the scope of patent protection?

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

### 6.2 What is the scope of copyright protection?

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

### 6.3 What is the scope of trade secret protection?

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

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

In China, the laws currently applicable to academic technology

transfers include the Law on Scientific and Technological Progress of the PRC (revised in 2021), the Law on Promoting Transfer and Commercialisation of Scientific and Technological Achievements of the PRC (revised in 2015) and Several Provisions on the Implementation of the Law on Promoting Transfer and Commercialisation of Scientific and Technological Achievements of the PRC issued by the State Council of the PRC in 2016. Such laws and regulations have adjusted previous policies in this field and clarified that the project undertakers, on the premise of no conflict with national security or national/public interests, are legitimately authorised to own relevant intellectual property ("IP") rights arising from the government-funded projects. Furthermore, the project undertakers are encouraged to legally transfer and commercialise these IP rights in various ways. However, any transfer or exclusive license to an overseas company shall be approved by the project administration organisation.

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

### 6.5 What is the scope of intellectual property protection for software as a medical device?

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

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

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

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

Please refer to question 6.4.

## 7 Commercial Agreements

### 7.1 What considerations apply to collaborative improvements?

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

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

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

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

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

## 8 Artificial Intelligence and Machine Learning

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

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

### 8.2 How is training data licensed?

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

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

According to the existing effective laws and regulations, AI can neither be an author in the context of the Copyright Law, nor an inventor or designer in the context of the Patent Law. As a result, the existing laws and regulations do not cover this area. However, with the rapid development of AI technology, the legislation of intellectual property protection of AI-generated contents is an important issue which needs to be urgently addressed. Chinese academia has been holding discussions on this issue as well. However, to date there is no unified understanding or relevant legislative proposals.

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

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

## 9 Liability

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

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

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

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

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

### 9.2 What cross-border considerations are there?

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

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

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

## 10 General

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

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

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

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

Non-healthcare companies that plan to independently and directly engage in the digital health industry should first obtain the qualification licence for the corresponding business according to law. For example, those intending to provide online consultation, paid medical information and other services

and construct a medical big data Cloud-based platform through medical websites and apps, shall obtain the approval of regulatory agencies and the relevant qualification licences.

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

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

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

Apart from business models, business prospects and other commercial factors, VC and PE investors should also pay attention to key issues such as market-access requirements for the industry that the target company falls into, the business qualification and business licence, core technologies and key technicians, procedures for obtaining ownership of relevant intellectual property rights, hardware facilities and cybersecurity protection, etc.

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

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

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

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

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

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

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

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

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

**10.7 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.**

With the advent of the digital era, digital health has undoubtedly become a key area in the construction of digital China. However, the current construction of digital health in China is still in its infancy.

We believe that in the future, China's digital health industry may have the following development trends:

First, "data" and "networks" are the core components of digital health. In the future, China may incorporate the informatics digital construction of medical institutions and medical service into new infrastructure.

In addition, as an emerging medical industry, digital health will profoundly change the medical organisational forms and medical behavioural patterns. The traditional Chinese legal governance framework, government management systems and multi-party relationship of rights, responsibilities and interests need to be readjusted or supplemented. In the future, China may: strengthen and improve the research work of digital medical legislation; improve relevant legislation in light of China's own industrial characteristics and international development trend; formulate and improve the healthcare data construction, opening, sharing and trading systems; clarify the rights and obligations of each participant in digital health; strengthen algorithm governance; and improve the risk-sharing mechanism of digital healthcare, to ensure the healthy and sustainable

development of the digital health industry in China through legislation. In November 2022, the National Health Commission and three other departments jointly released the "14th Five-Year Plan" for National Health Informatisation, which proposed the overall goal of "by 2025, we will initially build and form a unified, authoritative and interconnected national health information platform support and security system, and basically achieve the full coverage of public health institutions and the national health information platform".

Meanwhile, digital health, as a new medical model and business form, has also created new regulatory issues such as information leakage and privacy protection. In order to solve relevant problems, China will establish a governance mode compatible with the sustainable and healthy development of the digital health industry, innovate a coordinated governance model, and build a collaborative, efficient, inclusive and prudent digital medical supervision mechanism.

At last, the development of the digital health industry has accelerated the flat development of the medical service system structure. It is an inevitable trend to explore multiple co-governance in the new medical service system. In the future, industry self-regulation, platform governance, patient and medical staff rights protection may become increasingly important.

**Cindy Hu** focuses on the areas of corporate M&A, corporate finance and compliance. She is heavily involved in the pharmaceutical and healthcare industry, and leads the pharmaceutical and healthcare team of East & Concord.
Cindy has routinely advised well-known Chinese state-owned and private enterprises, publicly listed companies, and PE/VC funds in the area of pharmaceuticals and healthcare. She was recognised as one of the Top 15 M&A Lawyers by *ALB China*, as well as one of the Client Choice: Top 15 Compliance Versatile Practitioners by *LEGALBAND*. She was also endorsed as a Leading Lawyer in Corporate M&A by *Asialaw Profiles* and China's Top Lawyers (Corporate and M&A) by *LEGALBAND* multiple times. In 2022, Cindy's team ranked on the list of Life Sciences and Healthcare in *The Legal 500* and Pharmaceuticals and Life Sciences in *Asialaw Profiles*. Cindy is widely published both in China and internationally.

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

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

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

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

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

**Jiaxin Yang** is the backbone member of the pharmaceutical and healthcare team of East & Concord, with extensive experience in M&A, compliance and risk control in the healthcare sector. She regularly provides support and advice for well-known Chinese state-owned and private enterprises, foreign invested companies, as well as private equity funds on projects concerning stem cell R&D, digital health, wearable medical devices, cybersecurity and data protection.

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

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

East & Concord Partners has a well-earned reputation as one of the largest and most comprehensive law firms in China. With more than 600 legal professionals, the firm advises multinational companies, publicly listed companies, privately owned companies, state-owned enterprises, foreign invested companies, government offices and public institutions on a wide range of areas. Headquartered in Beijing, the firm has eight offices strategically located throughout China. The firm has also established extensive cooperation with many well-known international law firms so as to satisfy the development need for economic globalisation.
With more than 20 years of experience, the firm has gained a leading position and earned clients' trust and recognition in areas including: banking and finance; M&A; anti-dumping and anti-subsidy; pharmaceutical and healthcare; infrastructure and project financing; intellectual property; government legal affairs; cybersecurity and data protection; and dispute resolution.

**en.east-concord.com**

天達共和律師事務所
East & Concord Partners

# ICLG.com

## Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group