Chambers
Global Practice
Guides

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

Digital Healthcare 2021

China
Alan Zhou, Charlene Huang and Jenny Chen
Global Law Office

practiceguides.chambers.com

Law and Practice

Contributed by:
Alan Zhou, Charlene Huang and Jenny Chen
Global Law Office see p.19

CONTENTS

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

1. DIGITAL HEALTHCARE OVERVIEW

1.1 Difference between Digital Healthcare and Digital Medicine

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

Digital healthcare usually refers to healthcare technologies developed based on information technologies used by and for the public in general, including healthcare management, disease awareness, telemedicine, online sale of pharmaceutical products and other healthcare-related activities conducted through digital platforms.

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

1.2 Regulatory Definition

Digital healthcare and digital medicine are not legal terms defined in PRC laws and regulations.

1.3 New Technologies

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

Generally speaking, for digital healthcare, key technologies may include big data that can be used in public health monitoring, healthcare cost control, and internet of things and related sensor technology, global positioning system (GPS) technology and 5G technology that enables smart home and elder care, hospital management, telemedicine, etc.

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

1.4 Emerging Legal Issues

The key emerging legal issues in digital health may include the following.

Regulatory Framework

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

- PRC physician practising laws and telemedicine-related regulations;
- PRC drug administrative laws and regulations in relation to online sale of pharmaceutical products;
- PRC advertising laws, etc.

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

Cybersecurity and Data Protection

As digital health naturally involves a large amount of personal data, especially that of a sensitive nature, the design and implementation of lifecycle protection of the data utilised in the context of digital health would need to be carefully considered.

Liability

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

1.5 Impact of COVID-19

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

Prior to the outbreak of COVID-19, most patients in China typically visited physical healthcare institutions such as public hospitals, private hospitals or clinics. However, due to the restriction on movement necessitated by the pandemic, there has been a rapid acceleration of the widespread adoption of digital technology in both the delivery of healthcare services, such as telemedicine, online appointments and patient monitoring, and in AI-assisted diagnosis and treatment.

A series of notices and opinions were issued in 2020 to encourage healthcare institutions to leverage telemedicine for the purpose of relieving the pressure on the offline delivery of healthcare services. In addition, based on public statistics, as of April 2021, the number of internet hospitals in China has reached more than 1,100, a figure triple that at the end of 2019.

Many healthcare institutions and AI technology companies have collaborated to enhance the use of computed tomography (CT) in the diagnosis of COVID-19 by using AI for detection and classification of COVID-19 based on CT scans, and for assessing disease severity.

2. DIGITAL HEALTHCARE AND CLIMATE CHANGE

2.1 Digital Healthcare and Public Health Dangers Related to Climate Change

Climate change may affect public health directly through increase of extreme weather such as heat waves, and indirectly due to change of ecosystems such as the expanded geographic distribution of pathogens. The impact of climate change on society may further affect the mental health of individuals.

From a broad perspective, digital healthcare is expected to help address climate change related public health issues by enabling people to better monitor their personal health status and obtain personalised treatment, thereby, among others, reducing cost of access medical resources, and assisting with providing possible early warnings of future public health emergencies.

3. HEALTHCARE REGULATORY ENVIRONMENT

3.1 Healthcare Regulatory Agencies

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

The National Medical Products Administration (NMPA)

The NMPA regulates drugs, medical devices and cosmetics in China, responsible for the safety supervision and management of the same from registration and manufacturing to post-market risk management. Technology and devices, including software if it falls into the scope of drug or medical device, is also subject to the regulation and supervision by the NMPA and its subordinate branches.

The National Health Commission (NHC)

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

The clinical application of medical technologies for the purpose of diagnosis and treatment (including AI-assisted diagnosis and treatment) by healthcare institutions and professionals, is also regulated by the NHC.

The National Healthcare Security Administration (NHSA)

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

3.2 Recent Regulatory Developments

Regulatory Developments on Telemedicine

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

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

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

In addition, the growth of internet-based diagnosis also boosted the demand for internet sales of medicine. Currently, internet sales of over-the-counter (OTC) drugs are allowed while relevant regulations on internet sales of prescription drugs are expected to be officially released in the near term.

Regulatory Developments on Electronic Medical Insurance

In August 2019, the NHSA issued the "Internet Plus" Medical Service Prices and Medical Insurance Payment Policy and launched the electronic medical insurance system, which regulates the prices and insurance policies to allow for internet-based healthcare services to be covered by China's medical insurance system.

Regulatory Developments on AI-Assisted Diagnosis and Treatment

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

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

Regulatory Developments on Cybersecurity and Data Protection

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

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

From a general perspective, draft versions of two important data protection laws, the PRC Personal Information Protection Law and the PRC Data Security Law, were released for public comment, which indicates the continuous strengthening of data protection.

3.3 Regulatory Enforcement

Currently, the key areas of regulatory enforcement in digital healthcare include cybersecurity and personal data protection.

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

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

In terms of personal data protection, relevant data protection authorities such as the Cyberspace Administration of China (CAC), the Ministry for Industry and Information Technology (MIIT) and the PSB have been actively enforcing personal data protection requirements across industries, including healthcare. Industry supervision authorities such as the NHC and the NHSA are also involved in those enforcement actions on healthcare institutions.

4. NON-HEALTHCARE REGULATORY AGENCIES

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

CAC

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

PSB

In terms of cybersecurity, the PBS is mainly responsible for enforcing the MLPS and investigating cybercrimes. With respect to digital healthcare, the PSB's involvement may include record filing for MLPSs completed by healthcare institutions including internet hospitals, conducting inspections related to MLPS on healthcare institutions, and investigating crimes related to digital healthcare, such as the infringement of personal data and illegal access to information systems.

MIIT

The MIIT is responsible for regulating information technology and communication industry, recording filing and approval of Internet Content Provider (ICP), and formulating policies and standards on data security, etc. In terms of digital healthcare, MIIT's involvement may include regulating related technology development, such as the development of and security requirements for AI technology. In addition, the MIIT is actively leading personal data protection campaigns on mobile applications, including apps used in the healthcare industry.

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

5. SOFTWARE AS A MEDICAL DEVICE

5.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technology

Definition and Regulatory Authorities

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

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

Classification of SaMD

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

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

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

Generally, SaMDs used for image processing, data processing, in vitro diagnosis, and rehabilitation, are classified as Class II devices, while most of the SaMDs used for assisting treatment (eg, formulating treatment plan) and for assisting diagnosis (eg, giving clinical diagnosis and treatment basis and/or advice) are classified as Class III devices.

Regulations on SaMDs

Registration and updates of SaMDs

Class II medical devices manufactured in China must register with medical product administration on a provincial level, Class II medical devices manufactured outside of PRC and Class III medical devices shall register with the NMPA. Software updates of SaMD could be divided into major updates and minor updates. Major updates refer to enhancement that affects the intended uses, environment of use or core function of medical devices. Minor updates refer to enhancement that does not affect the safety or effectiveness of medical devices as well as corrective updates.

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

Manufacturing, sale and use of SaMDs

Manufacturing and sales of SaMD are subject to corresponding licensing requirements. In addition, the clinical use of certain types of SaMD may be subject to additional regulations, eg, using AI-assisted diagnostic technology is subject to self-assessment and filing with the relevant health commission, and shall meet the specific rules applicable to the clinical use of such technology.

6. TELEHEALTH

6.1 Role of Telehealth in Healthcare

Internet Hospital

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

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

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

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

In terms of online prescription, regulations and policies have been issued on facilitating circulation of electronic prescriptions issued in internet-based medical services to retail pharmacies, and on allowing internet sales of prescription drugs, with implementation rules on both expected to be released in the near term.

Family Doctor Contracting Services

Family doctor contracting services are mainly provided by community healthcare institutions. After signing a family doctor service agreement with residents, family doctors provide relevant services according to the requirements of the agreement, which may include health management services, health consultation services, outpatient services, drug delivery and medication guidance services, etc. The residents could make appointment through online channels such as websites and apps.

Third-Party Information Platform

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

Cross-Border Telemedicine

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

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

6.2 Regulatory Environment

For telemedicine, the NHC issued a series of notices and opinions in 2020 to encourage healthcare institutions to leverage telemedicine to release the pressure of offline delivery of healthcare services. Although there has been a rapid acceleration of telemedicine, some gaps and issues remain to be resolved and clarified from a national policy perspective, such as the expansion of the scope of internet-based diagnosis and treatment, and the application of internet-based diagnosis and treatment on first-time visits, etc.

6.3 Payment and Reimbursement

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

7. INTERNET OF MEDICAL THINGS

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

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

Life cycle monitoring of medical devices

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

Intelligent operating rooms

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

Wearable health monitoring devices

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

Technological Developments That Drive the Internet of Medical Things

5G networks

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

NB-IoT

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

Sensors

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

Regulatory issues for the IoMT

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

8. 5G NETWORKS

8.1 The Impact of 5G Networks on Digital Healthcare

The Impact of 5G Networks

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

In areas such as remote monitoring, remote analysis, remote control and remote diagnosis, where data is collected from various sources in disorder format, 5G networks also helps to solve the issues of data sharing and cleaning to support the development and application of AI technologies.

The Commercial and Contractual Considerations of Healthcare Institutions

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

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

9. DATA USE AND DATA SHARING

9.1 The Legal Relationship between Digital Healthcare and Personal Health Information

Key Legal Issues in Using and Sharing Personal Health Data

Under the PRC data protection framework, general privacy laws and regulations such as the PRC Cybersecurity Law, the PRC Civil Code the PRC Personal Information Protection Law (a draft of which is expected to be officially promulgated soon) regulate the protection of personal data and set up the fundamental principles and general requirements, while the healthcare regulation of personal health information provides more specific protection requirements on healthcare data.

Defining personal health data

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

Broad data requirements

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

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

Consent

In terms of consent, digital healthcare has not yet substantially changed the nature of patient consent, instead, it could provide more alternative means to obtain consent from the perspective of service providers. Informed consent requires a data controller to provide a holistic view regarding the scope and purpose of data collection, use, share, transfer and retention, based on which the data subject could provide a voluntary consent through an active conduct. In practice, consent is frequently obtained through clicking on the consent button of a terminal device by a data subject, handwritten signatures by a data subject in both electronic and paper format, as well as recording the oral expression of consent made by a data subject.

Legal Considerations in Sharing Personal Health Data

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

- Restriction on sharing – whether there are any restrictions imposed by PRC laws that prohibit sharing of specific categories of personal health data, eg, Human Genetic Resources (HGR), including HGR materials and HGR information, are not allowed to be shared with external parties without explicit approval from relevant authorities.
- Cross-border data transfer – whether the personal health data would fall into the scope of certain types of data that are required to be stored within the territory of China and are subject to security assessment and approval before being exported to other jurisdictions.
- Informed consent – whether informed consent from the data subject is properly obtained and whether special circumstances under which consent is not required are met.
- Necessity and legitimacy – whether such sharing of personal health data is conducted based on necessity and to achieve legitimate purposes.
- Data security – whether adequate security measures are designed and implemented for the data sharing.
- Due diligence on transferee – whether proper due diligence process is completed on the capability of the transferee to ensure data security of the personal health data.
- Contractual agreement – whether contractual agreement that stipulate the respective rights and obligations (including but not limited to security obligations of the transferee, scope of use by transferee, restriction on sharing, retention period and disposal requirements, assumption of liabilities for data breach) is concluded between the transferor and transferee.

Liabilities

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

- criminal liabilities for infringement of personal data include criminal detention, fixed-term sentence and monetary fines depending on the severity of the conduct and consequence;
- administrative liabilities for illegally processing of personal data include written warnings, confiscation of illegal gains, monetary fines (ten times of the illegal gains or fines up to RMB1 million), suspension of business, and revocation of business licences under serious circumstances (note: the draft version of the PRC Personal Information Protection Law proposes to raise the monetary fines to 5% of the business operator's annual turnover of previous year); and
- civil liabilities for infringement of personal data could be divided into torts liabilities and liabilities for breach of contract.

10. AI AND MACHINE LEARNING

10.1 The Utilisation of AI and Machine Learning in Digital Healthcare

AI, Machine Learning and Data Security Concerns

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

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

Likewise, there are strengths and weaknesses of a centralised electronic health record computer system. Strengths include better integration of healthcare resources and more efficient and effective delivery of healthcare services, while the weaknesses would still be the concerns for data security, especially when the centralised nature of the electronic health record computer system makes the whole system and data more vulnerable to cyber-incidents or cyber-attacks.

Data Use and Data Sharing in the Machine Learning Context

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

- Informed consent – the data controller would need to obtain informed consent from the data subjects for data collection, use and sharing.
- Data security – the data controller would need to ensure adequate security measures are designed and implemented for data use and sharing.
- Engagement with data processors – if the data controller engages third-party data processers to process the user data, such as data tagging, the data controller would need to ensure that the data processor would only process the data within the aligned scope and would implement adequate data security measures through due diligence, contractual agreements and/or data audits.

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

Natural Language Processing

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

11. UPGRADING IT INFRASTRUCTURE

11.1 IT Upgrades for Digital Healthcare

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

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

Looking forward, a solid foundation for digital healthcare or "Internet Plus healthcare" could be established through data management and integration of various data resources, unification and standardisation of data resources models, integration of healthcare services and platforms, elimination of information gaps among departments of the healthcare institution, to achieve the goals of resource sharing and business collaboration of healthcare services, supply of medical products, medical insurance and comprehensive management.

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

11.2 Cloud Computing

Key factors in driving the increase of cloud computing in healthcare include the following.

- Data storage – according to the NHC, data storage is required to establish national and municipal platforms, and establish corresponding data backup systems, which can withstand the pressure of the extensive data storage required for healthcare services.
- Data processing and computing power – the demand for data processing and computing power is increased due to the integration of various information systems.
- System maintenance – more maintenance resources are required where the IT systems are set up and operated independently by different healthcare institutions.

Key legal concerns in using cloud computing include the following.

- Data security and privacy – users upload the data to the cloud, which is managed and controlled by the cloud service provider, while not directly controlling the cloud computing system. This leads to the issue of separation between ownership and control, resulting in users relying on the security and internal control of the cloud service provider.
- Cross-border data transfer – under the applicable PRC laws and regulations, certain types of data, such as healthcare big data and population health information, are required to be stored within the territory of China and are subject to security assessment and approval before being exported to other jurisdictions. As the data is stored in the data centre of the cloud service provider, when there is any change of infrastructure planning, especially for those service providers which set up data centres in multiple jurisdictions, there is a risk of illegal cross-border data transfer.

Sensitive Data

As healthcare services involve a large scale of sensitive data, the practice for use of cloud services for data centre infrastructure would vary depending on types of the involved data. For healthcare institutions, the most sensitive data, such as HGR information, would usually be stored locally within total control of the institutions. As for other data, private cloud services would be preferred due the higher security level compared with public cloud services. And in terms of the selection of cloud service provider, the criteria mainly include:

- whether it has completed the MLPS under the PRC laws; and
- whether data localisation could be achieved.

IT Upgrades

It is a common practice that IT vendors outside the healthcare industry would provide the technology upgrade, or sometimes multiple IT vendors would be involved in IT upgrades and maintenance; therefore, in terms of vendor management, proper measures would be suggested such as pre-engagement due diligence, stipulation of data security obligations and regular data security audits, to exercise more control over the external vendors.

12. INTELLECTUAL PROPERTY

12.1 Scope of Protection

Scope of Protection of Intellectual Property Rights

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

Patent

The PRC Patent Law protects invention, utility model or design that possesses novelty, creativity and practicality. Under the PRC Patent Law:

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

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

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

Copyright

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

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

Trade secrets

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

Protection of Data

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

AI Inventorship and Authorship

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

12.2 Research in Academic Institutions

Copyright Allocation

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

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

Patent Right Allocation

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

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

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

12.3 Contracts and Collaborative Developments

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

13. LIABILITY

13.1 Patient Care

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

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

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

In terms potential bias issue of AI, as bias would likely be deemed as ethical issue, the application of AI with ethical issues is currently restricted or profited.

13.2 Commercial

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

14. HOT TOPICS AND TRENDS ON THE HORIZON

14.1 Hot Topics That May Impact Digital Healthcare in the Future

Another important hot topic that may or is already impacting digital healthcare is blockchain technology. As critics often complain about the privacy concerns arising from telemedicine or internet hospitals, blockchain technology could be used to promote the secured sharing and distribution of healthcare data.

In October 2020, the NHC issued the Opinions on Strengthening the Construction of a Standardized System of Health Information, which clarifies the trend of exploring the application of blockchain technology in the healthcare industry. This includes exploring and researching blockchain application scenarios in healthcare, accelerating research and developing blockchain information service standards in healthcare, and strengthening norms to guide the integration of blockchain technology and healthcare industry applications.

Under these policies, healthcare institutions are encouraged to explore the application of blockchain technology in medical consortia, personal health records, electronic prescriptions, drug management, medical insurance, smart hospital management, vaccine management, gene sequencing, etc, on the premise of data safety. In practice, internet hospitals are launching pilot programmes for implementing and integrating blockchain technologies.

Despite the above, there are still rising doubts about the security and effectiveness of the technology and its application in the healthcare industry, which need to be further analysed and verified in the process of the exploration.

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

Global Law Office was one of the first law firms in the People's Republic of China (PRC) and is one of the largest, with more than 465 lawyers practising in its Beijing, Shanghai, Shenzhen, and Chengdu offices. Its life sciences and healthcare (L&H) practice group is one of the leading advisers in China, having provided "one-stop" legal services for every area of the L&H industry, including drug R&D, clinical research organisations, pharmaceuticals, biotechnology, medical devices, supply producers and distributors, hospitals and other healthcare provider and investment funds. Global advises clients on challenging L&H legal issues such as regulatory compliance, structuring transactions and contractual arrangements, realisation of pipeline and geographic expansions, capital-raising and project-financing, M&A, re-organisations, IP protection, licensing and distribution arrangements, settlement of disputes involving adverse effects in clinical trials and medical treatment. The firm has close links to industrial associations and makes recommendations on industry codes of conduct and compliance management standards.

AUTHORS

Alan Zhou is the leading partner based in Global Law Office's Shanghai office, and has a strong background in the life sciences and healthcare (L&H) practice. Alan has routinely represented multinational corporations, well-known Chinese state-owned and private enterprises, and private equity/venture capital funds in the L&H area. Alan has been engaged by local authorities and industrial associations to advise on legislation and industrial standards in the L&H industry, areas of which include e-healthcare, medical insurance reform, medical representative administration, and other compliance issues. Alan has won numerous awards and has been recognised by peers for his expertise. Alan is widely published both in China and internationally.

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

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

Global Law Office

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

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

环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979