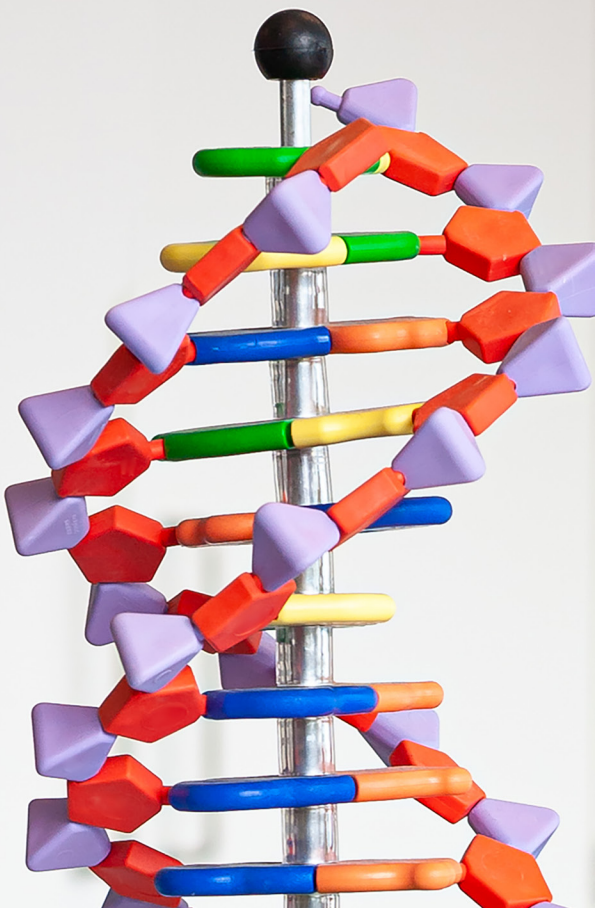
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Digital Healthcare 2025

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



China: Law & Practice

Alan Zhou, Charlene Huang, Jenny Chen and Stephanie Wang
Global Law Office

CHINA

Law and Practice

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

Contents

Global Law Office was one of the first law firms in the People's Republic of China (PRC) to have more than 600 lawyers practising in its Beijing, Shanghai, Shenzhen and Chengdu offices. Its life sciences and healthcare (L&H) group, also known as China Life Sciences and Healthcare Law (CLHL), is one of the leading practice groups in China. It provides "one-stop" legal services for every sector in the L&H industry, including R&D, clinical research organisations, pharmaceuticals, biotechnology, medical devices, supply producers and distributors, hospitals and other healthcare providers as well as investment funds. The firm regularly advises clients on challenging L&H legal issues such as regulatory compliance, structuring transactions and contractual arrangements, realisation of pipeline and geographic expansions, capital raising and project financing, M&A, reorganisations as well as 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 in the life sciences and healthcare practice group at Global Law Office. He has a strong background in the area, routinely representing multinational corporations, well-known Chinese state-owned and private enterprises and private equity/venture capital funds. As a participant or an external counsel, he has been engaged by local authorities and industrial associations to advise on legislation and industrial standards in the life sciences and healthcare industry, including guidelines on compliance and risk control, e-healthcare, medical insurance reform and medical representative administration. His insights have been widely published at home and abroad.

Charlene Huang is a partner and is based in Global Law Office's Shanghai office. She has in-depth experience in M&A and cross-border licence deals, especially in the healthcare and life sciences sector. She has led projects involving outbound and inbound investment, acquisition of state-owned and private equity/assets, pipeline consolidation or restructuring of multinational corporations 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. She also has in-depth experience in advising multinational companies in general corporate, cybersecurity and data management matters.

Jenny Chen is a partner and is based in Global Law Office's Shanghai office. She is an attorney-at-law in the PRC and California in the US. She is also a certified fraud examiner at the US ACFE and is a certified (but non-practising) public accountant. She focuses her practice on compliance, government investigation, internal investigation and data security. She is well-versed in conducting investigations in connection with anti-corruption under the US FCPA and the UK Bribery Act as well as financial frauds, occupational embezzlement, self-dealing and trade secrets. She 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.

Stephanie Wang is an of counsel and is based in Global Law Office's Shanghai office. She has been actively involved in advising multinational pharmaceutical and medtech companies on their corporate governance, daily operations and compliance. She has extensive knowledge of, and experience, in the life sciences and healthcare industry and routinely advises clients on a variety of commercial agreements relating to R&D, licensing, marketing authorisations and the manufacturing, distribution and promotion of medical products. She has also worked with notable private equity institutions on investments in various pharmaceutical enterprises.

Global Law Office

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

Tel: +86 212 310 8200
Fax: +86 212 310 8299
Email: Alanzhou@glo.com.cn
Web: www.glo.com.cn

环 球 律 师 事 务 所
GLOBAL LAW OFFICE

1. Digital Healthcare Usage

1.1 Types of Digital Healthcare

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.

Alongside digital healthcare, digital medicine usually refers to the application of IT in the process of diagnosis and treatment, which can only be performed by qualified medical institutions.

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

1.2 Use/Application of Digital Healthcare

Digital healthcare is widely used in healthcare settings in China, especially in terms of the following.

Software as a Medical Device (SaMD)

When a software product processes medical device data and its core function is to manage, measure, model, calculate or analyse this data for medical purposes, the product falls within the scope of a SaMD.

Self-Care, Wellness and Fitness IT Products

If a preventative care concerns general healthcare consulting, elder care, nursery, massage, fitness or wellness, without making judgement about diseases or giving targeted recommendations towards specific health issues or conditions, it may not fall within the definition of diagnosis and treatment and will therefore not be subject to special regulation. However, if a preventative care falls within the area of diagnosis or treatment activities (eg, disease screening or vaccination), it can only be performed by a qualified doctor in a medical institution.

Artificial Intelligence (AI) and Machine Learning

Unlike traditional medical devices, the development of an AI medical device may need a tremendous amount of data for machine learning and training. Companies engaging in new digital healthcare technologies should be aware of the relevant regulatory and legal issues (including cybersecurity and data protection). They should also be aware that they will be subject to the same requirements.

Telemedicine

Internet hospitals, as a major telemedicine model, can be divided into two categories:

- internet hospitals associated with specific offline healthcare institutions, eg, an internet hospital of a particular public hospital; and
- independent online hospitals set up with reliance on offline healthcare institutions, eg, an internet hospital set up by internet companies together with public hospitals.

Under both categories, internet hospitals may provide internet-based diagnosis and treatment to patients, which are limited to the follow-up

diagnoses of certain common and chronic diseases.

Cybersecurity and Data Protection

As digital healthcare involves a large amount of personal data, especially that of a sensitive nature, the design and implementation of life cycle protection of this data needs to be carefully considered under the cybersecurity and privacy protection laws and regulations, particularly the regulations of the Personal Information Protection Law of the PRC (the "PIPL"), which came into effect on 1 November 2021.

1.3 Benefits of Digital Healthcare

The advantages of digital healthcare could generally be summarised as:

- improved accessibility and efficiency;
- customised and precise medicine fulfilment; and
- the promotion of patient engagement and transparency.

With proper support of digital healthcare, patients could be provided with e-consultation services in qualified third-party platforms with subsequent time saving benefits.

From the perspective of healthcare professionals, AI-assisted diagnostic tools, multi-disciplinary consultations and e-medical record systems could largely improve the efficiency and collaboration in the work practice.

Although investment in the digital infrastructure would be considerable in the early implementation stage, the application of digital healthcare could optimise resources and avoid unnecessary treatments which could largely reduce the cost of patients and healthcare institutions. With this technology, the telemedicine platform can automatically collect various vital signs data, upload the data to the hospital control centre and analyse the data in real time, to provide doctors with an early warning and allow telemedicine services to be provided.

2. Legal Framework

2.1 Definition of Digital Healthcare

Digital healthcare is not legally defined in the laws and regulations of the PRC but is frequently referred to in commercial contexts and industry policies (see **1.1 Types of Digital Healthcare**). Despite this, if any service or product in the fields of digital healthcare and digital medicine falls within the category of pharmaceuticals or medical devices or is going to be used for the diagnosis and treatment of human diseases, administrative regulations will apply accordingly.

2.2 Laws and Regulations

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

- physician practising laws and telemedicine-related regulations in the PRC;
- drug administrative laws and regulations in relation to online sale of pharmaceutical products in the PRC;
- advertising laws in the PRC;
- laws and regulations on cybersecurity and data protection in the PRC; and
- laws, regulations and industry standards on telecommunications and IT in the PRC.

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

2.3 Role of Policymakers

China's legal framework encourages the implementation of digital healthcare while balancing development and risk with regulation specifically in the following ways.

SaMD

Under the applicable laws and regulations in the PRC, standalone software as a SaMD refers to software that:

- has one or more medical uses;
- does not require medical device hardware to achieve the intended use; and
- runs on a common computing platform.

A SaMD can be used together with multiple medical devices or a specific medical device.

Like other medical devices, SaMDs are regulated by the National Medical Products Administration (the "NMPA") and its subsidiary branches, including research and development, registration, manufacturing, sales, post-market risk management, adverse event reporting, etc.

In terms of a software product that uses AI, whether it is administrated as a SaMD or not depends on its intended use, processing object and core function, among other things. When a software product processes medical device data and its core function is to manage, measure, model, calculate or analyse this data for medical purposes, the product falls within the scope of a SaMD.

Registration of a SaMD

Medical devices in China are classified into three categories. There are different registration procedures for each based on their potential risk to patients. According to the current Medical Device Classification Catalog (the "Catalog") issued by the NMPA, SaMDs listed in the Catalog are classified as Class II or Class III medical devices. Class II products manufactured in China must be registered with the provincial medical products administrations, while Class III products and the imported Class II products must be registered with the NMPA.

Software updates of SaMDs can be divided into major and minor updates. Major updates refer to enhancements that affect the intended use, environment of use or core function of medical devices. Minor updates refer to enhancements that do 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 next registration application for post-market change or renewal. In those cases where software employs self-adaptive learning or continuous learning, users also assume the role of product developer and share the product quality responsibility and legal responsibility with the registration applicant.

Given the existing law and regulation framework and technological capacities, the self-learning function of software designed with continuous learning or self-adaptive learning capacity should therefore either be disabled, or if enabled, not utilised.

Manufacturing, Sale and Use of SaMDs

The manufacturing and sale of SaMDs are subject to corresponding licensing requirements, specifically the Appendix for SaMDs of Good Manufacturing Practice for Medical Devices. In addition, the clinical use of specific types of SaMDs may be subject to additional regulations, eg, using AI-assisted diagnostic technology is

subject to self-assessment and filing with the relevant health commission and must meet the specific rules applicable to the clinical use of the technology.

Telemedicine

In 2020, the National Health Commission (the "NHC") issued a series of notices and opinions to encourage healthcare institutions to leverage telemedicine and alleviate the pressure on offline delivery of healthcare services. In March 2023, the General Office of the Central Committee of the Communist Party of China and the General Office of the State Council issued opinions emphasising that expanding the coverage of telemedicine and establishing a telemedicine collaboration network was essential to improve the medical and healthcare service system.

According to the Key Tasks in 2024 for Deepening the Reform of Medical and Healthcare Systems announced by the General Office of the State Council, telemedicine could contribute to the capacities of primary-level medical and healthcare services.

Furthermore, in April 2025, the NHC, together with other authorities, issued the Guiding Opinions on Optimising the Layout and Construction of Primary-level Healthcare Institutions (the "Guiding Opinions"). The Guiding Opinions outline a three phase goal over the next ten years and aim to realise the basic popularisation of telemedicine and smart health services by 2030.

Family doctor contracting services are currently mainly provided by community healthcare institutions, demonstrating the advantages of telemedicine in primary healthcare. After signing a family doctor service agreement with residents, family doctors provide relevant services according to the requirements of the agreement, which may include health management services, health consultation services, outpatient services, rehabilitation, smart aided therapeutics and medication guidance services, etc.

Residents can execute service agreements, make appointments and accept health consultations and follow-up visits of chronic diseases through online channels such as websites and apps.

AI and Machine Learning

AI use and development in healthcare is progressing rapidly in China and has been playing a robust and increasing role in the healthcare industry. Since 2016, with the strong support of national policies, China's giant technology companies have entered this field and launched different types of AI products.

From a regulatory perspective, the NMPA issued the Guiding Principles for the Review of Registration of AI Medical Devices in 2022, to regulate the registration of AI products as medical devices. As the most common form of AI, machine learning is widely applied in various aspects such as AI-assisted diagnostics and treatment, medical imaging, precision medicine and pharmaceutical research. These are followed by data security concerns with respect to the protection of large-scale personal sensitive data and cyber-attacks.

The Provisions on the Management of Deep Synthesis in Internet Information Services and the Interim Measures for the Management of Generative AI Services, which respectively came into force on 10 January 2023 and 15 August 2023, set out boundaries for applying AI technology and offering related services, emphasising that innovative development is as important as

safeguarding national security and public interest.

In terms of the industry-specific regulations, the Measures for the Review of Sci-tech Ethics (for Trial Implementation), effective as of 1 December 2023, specify that the entities engaged in the life sciences, medicine, AI and other scitech activities will set up a scitech ethics (review) committee if their research involves sensitive fields of scitech ethics. In addition, in December 2024, the General Office of the State Council issued the Opinions on Comprehensively Deepening the Reform of Drug and Medical Device Regulation and Promoting the High-Quality Development of the Pharmaceutical Industry. The Opinions encourage the optimisation of the medical device standard system and support the research and establishment of standardisation technology organisations for cutting-edge medical devices, such as AI and medical robots.

Elsewhere, according to the 2025 Legislative Work Plan of the Standing Committee of the National People's Congress, the legislative projects on governing online illegal activities and the healthy development of AI are at a preparatory stage.

Cybersecurity and Data Protection

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

- maintain grading mechanisms for both cybersecurity and data security;
- enhance the encryption management;
- carefully keep a system security log;
- carry out periodic cybersecurity monitoring and early warning checks;
- establish security incident reporting and response procedures; and
- formulate emergency response plans.

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

2.4 Technical Standards

No information has been provided in this jurisdiction.

2.5 Issue-Specific Legal Framework

No information has been provided in this jurisdiction.

2.6 Sufficiency of Legislative Framework

No information has been provided in this jurisdiction.

3. Regulatory Oversight

3.1 Oversight of Digital Healthcare

Various health regulatory authorities are involved in regulating digital healthcare technologies. They include the following national authorities (and their subordinate branches as applicable).

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

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

Additionally, 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 supervised by the NHC.

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

3.2 Non-Healthcare Regulatory Bodies
Certain aspects of digital healthcare fall within the remit of other non-healthcare regulatory bodies. These are as follows.

The Cyberspace Administration of China (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 collection and utilisation of personal information, cross-border transfer of healthcare data and the cybersecurity review of internet hospitals, etc.

The Public Security Bureau (PSB)
In terms of cybersecurity, the PSB is mainly responsible for enforcing the Multi-Level Protection Scheme (the "MLPS") and investigating cybercrimes. With respect to digital healthcare, the PSB's involvement includes:

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

The Ministry for Industry and Information Technology (MIIT)
The MIIT is responsible for:

- regulating the IT and communications industry;
- recording filing and approval of internet content providers (ICPs); and
- formulating policies and standards on data security, etc.

In terms of digital healthcare, the MIIT's involvement may include regulating technology-related developments, such as the development of, and security requirements, for AI technology. Additionally, the MIIT actively leads personal data

protection campaigns on mobile applications, including apps used in the healthcare industry.

National Data Bureau (NDB)

The NDB was officially inaugurated on 23 October 2023 to co-ordinate the improvement of data infrastructure systems, including the development, utilisation and interaction of data resources and pushing the building of digital China forward. It is therefore expected that the NDB will play a specific role in data protection enforcement regarding digital healthcare.

3.3 Enforcement

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

In terms of cybersecurity, the implementation of the MLPS, which is a compulsory legal obligation under the Cybersecurity Law of the PRC and relevant regulations, is now becoming an enforcement focus for most industries involving sensitive information, particularly healthcare.

The MLPS is composed of a series of technical and organisational standards and requirements that need to be fulfilled by all network operators in China. As the development and operation of digital healthcare heavily relies on networks and IT infrastructure, it is critical for digital healthcare providers to enforce and complete the MLPS grading process.

Under the Administrative Measures for Internet-based Diagnosis (for Trial Implementation) and the Administrative Measures for Internet Hospitals (for Trial Implementation), healthcare institutions providing internet-based diagnosis services and internet hospitals will be graded and protected as Grade III under the MLPS regime. Failure to complete the MLPS will lead to administrative penalties including warnings and fines being issued by the PSB.

In terms of personal data protection, relevant data protection authorities such as the CAC, the 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.

3.4 Sufficiency of Oversight

No information has been provided in this jurisdiction.

4. Liability

4.1 Legal Risks of Digital Healthcare

Data Use and Data Sharing

As personal health data largely falls within the category of personal sensitive data under the laws of the PRC, the scope of liability for data breach or unauthorised use of, or access to, personal health data in use and sharing are currently the same as for personal data. They are regulated under the Criminal Law of the PRC, the Cybersecurity Law of the PRC, the PIPL, the Regulations on the Security Management of Network Data and the Civil Code of the PRC, which include:

- criminal liabilities for infringement of personal data including criminal detention, a fixed-term sentence and monetary fines depending on the severity of the conduct and the consequences;
- administrative liabilities for illegally processing personal data including written warnings,

confiscation of illegal gains, monetary fines (up to RMB50 million or 5% of the turnover of the previous year), suspension of business and, in serious circumstances, the revocation of business licences;
- personal liabilities imposed on the person in charge including fines of up to RMB1 million and prohibition from holding certain positions; and
- dividing civil liabilities for infringement of personal data into tortious liability and liability for breach of contract.

Patient Care

With respect to the determination of liabilities in the event injury is suffered by a patient using a SaMD, provisions on product liability and tort will generally apply, ie, the patient can claim compensation from either the manufacturer or the seller if the injury is caused by a product defect. Where the party (either the manufacturer or the seller) compensating the patient is not liable for the defect, they may recover their losses from the other.

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

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

In terms of the potential AI bias issue, bias will likely be considered an ethical issue. This will be further clarified by enforcement practice.

Commercial Liabilities

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

4.2 Liability Frameworks

The prohibitions and corresponding legal liabilities for misconduct are mainly governed by the Criminal Law for criminal liabilities in the PRC, the Cybersecurity Law in the PRC, the PIPL and the Regulations on the Security Management of Network Data for administrative liabilities as well as the Civil Code for civil liabilities in the PRC (see **4.1 Legal Risks of Digital Healthcare**).

The specific legal liabilities arising from the use of telemedicine platforms depend on their functions and usage. If a telemedicine platform is aimed at providing health education or caring services rather than medical services, the user may file a claim for liability against the owner of the platform.

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

4.3 Defences

China employs comprehensive and inclusive laws and regulations to systematically manage digital healthcare risks and to keep up with technological advancements, particularly in terms of data security and product liability, especially in terms of:

- data security and privacy protection mechanisms;
- classifications and regulatory approval of AI medical software;
- online sales supervision;
- internet diagnosis and treatment management;
- e-medical records application; and
- ethics review, etc.

5. Emerging Legal Issues and Reform

5.1 Emerging Legal Issues in Digital Healthcare

Regulatory Developments on Telemedicine

"Internet Plus Healthcare", ie, healthcare combined with the application of the internet, is now a key national strategic priority in China. To regulate diagnosis and treatment provided remotely, ie, teleconsultation by healthcare professionals or internet-based diagnosis, the NHC and the National Administration of Traditional Chinese Medicine (the "NATCM") in July 2018 issued the:

- Administrative Measures for Internet-based Diagnosis (for Trial Implementation);
- Administrative Measures for Internet Hospitals (for Trial Implementation); and
- Good Practices for Telemedicine Services (for Trial Implementation).

The NHC and the NATCM also released the Rules for the Regulation of Internet-based Diagnosis (for Trial Implementation).

These measures clarify how technical support on internet-based diagnosis and treatment should be conducted and set out the regulatory requirements to do so.

In addition, the growth of internet-based diagnoses also boosted demand for online medicine sales. The Provisions for Supervision and Administration of Online Drug Sales and the Circular on Regulating the Display of Online Sales Information of Prescription Drugs, which were enacted in recent years, state that, except for medicinal products subject to special administration, internet sales of over-the-counter drugs and prescription drugs are allowed. Nevertheless, it is crucial for third-party platforms and enterprises engaging in online drug sales to comply with the relevant requirements for displaying information about the online sales of prescription drugs.

Regulatory Developments on E-Medical Insurance

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

In September 2024, the NHSA issued the Announcement on Further Improving the Collection of Medical Insurance Drug and Consumables Traceability Code Information (the "Announcement"). The Announcement clarified

that the NHSA is developing a nationally unified interface for the production and circulation enterprises of drugs and consumables to upload traceability code information, so as to achieve one-time uploading with nationwide applicability.

The NHSA plans to establish a comprehensive three-code mapping database to link traceability code, medical insurance code and then commodity code to reduce the burden of code scanning.

Regulatory Developments on AI-Assisted Diagnosis and Treatment

In terms of AI, China's overall legal framework is still developing. There is currently a lack of specialised laws and administrative regulations dedicated to AI. The main regulation in force is the Interim Measures for the Management of Generated AI Services which was jointly issued by seven ministries on 15 August 2023 and other relevant departmental regulations (see **2.3 Role of Policymakers**).

In addition, as early as 2017, the State Council released the Development Plan for a New Generation of AI, setting a strategic goal of initially establishing AI laws, regulations, ethical norms and policy systems to form AI safety assessment and control capabilities by 2025. Since then, the State Council, various ministries and specific local governments have issued a series of policies, regulatory documents and local regulations addressing AI governance and development.

Between 2022 and 2024, a series of AI-related national standards were released one after another.

In April 2025, the MIIT and six other ministries jointly issued the Implementation Plan for Digital and Intelligent Transformation of the Pharmaceutical Industry (2025-2030). One of its key tasks for the next five years is the "Digital and Intelligent Technology Empowerment Initiative", which includes:

- strengthening the development and application of digital and intelligent products for the pharmaceutical industry;
- integrating and releasing the value of pharmaceutical data elements;
- transforming and upgrading information infrastructure; and
- deepening the application of AI empowerment.

Regulatory Developments on Data Protection

In July 2018, the NHC issued the Administrative Measures on the Standards, Security and Services regarding National Healthcare Big Data (the "Administrative Measures"). The Administrative Measures specified the direction of travel for 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 on how to protect healthcare data, particularly considering the rapid development of digital healthcare.

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

From a general perspective, following two important data protection laws which took effect in 2021 (the PIPL and the Data Security Law of the PRC), a series of measures and guides have been promulgated since 2022 regarding detailed regulations on data protection, security assessment measures and the execution of standard contracts for cross-border data transfer.

Human genetic resources (HGRs) are primarily governed by the Biosecurity Law, the Administrative Regulation on Human Genetic Resources (the "HGR Regulation") and the implementation rules issued in 2023. Foreign parties with established or controlled entities in the PRC are only permitted to use Chinese HGR upon filing/approved by the HGR authority and are prohibited from collecting, storing and making cross-border transfers of the HGR.

The NMPA issued Implementation Measures for the Protection of Drug Trial Data (for Trial Implementation) for public comment in March 2025, aimed at optimising the protection framework for drug trial data further. The aim was to encourage the research and development of innovative drugs and accelerate pharmaceutical innovation.

5.2 Recent or Imminent Reform

Pharmaceutical companies have recently shown an increasing dependence on digital tools when engaging with healthcare professionals and patients. Data collection via digital tools serves as a key element in analysing healthcare professionals' and patients' perceptions of treatment alternatives and drug dosage, market share, etc. These data collection activities are associated with a variety of risks and are subject to regulatory supervision.

Personal Data Protection

According to the laws in the PRC, healthcare institutions and professionals have to protect the personal data and privacy of patients. For pharmaceutical companies processing the personal data of patients, informed consent typically serves as the legal basis. An individual or entity that illegally processes personal data incurs administrative or criminal liabilities. Pharmaceutical companies commonly and strictly prohibit their employees from illegally collecting or further using or sharing the personal data of patients, thereby preventing liabilities (see **4.1 Legal Risks of Digital Healthcare**).

Digital patient management programmes

Pharmaceutical companies often have to engage vendors to establish and maintain platforms on smartphone applications or WeChat mini programmes. The primary purpose of these digital patient management programmes is to assist healthcare professionals in optimising patient management. These programmes typically involve the collection of detailed personal information from patients, such as diagnosis results, dates of visits, medical histories, treatment responses and other health-related data. This comprehensive data collection is achieved by providing digital platforms where both patients and healthcare professionals can log information, track the treatment process in real time and communicate effectively.

However, when vendors neglect to provide patients with sufficient information regarding how their personal data will be collected, stored, processed and shared and therefore fail to obtain legally required consent, significant risks of personal data infringement are created. Given that these vendors are entrusted by pharmaceutical companies, any non-compliance or data-related mishandling may result in the transfer of these

risks directly to the pharmaceutical companies, potentially leading to legal liabilities, reputational damage and loss of patient trust.

In addition to the risk emanating from vendors, pharmaceutical companies also face concerns related to improper employee actions. If employees deviate from internal policies during the execution of the digital patient management programme, by collecting personal information without consent or by misusing the data collected through the platforms, for example, it can expose pharmaceutical companies to legal consequences for the unlawful processing of personal data.

These violations not only undermine the integrity of the patient management programme but also pose a threat to the privacy and rights of patients, further highlighting the need for strict oversight and compliance within the pharmaceutical industry's digital operations.

Internal work report

Pharmaceutical companies typically require medical representatives to visit healthcare professionals and document interactions through internal digital systems to track work progress. During these visits, if medical representatives collect patients' personal information (eg, names, diagnoses, treatment outcomes, follow-up plans) and record it in the system, this poses significant risks.

Patient data collection in these situations is often framed as part of sales or marketing efforts (eg, visualising patient journeys from the seeking of treatment to drug purchase) but medical representatives are primarily responsible for documenting healthcare professional interactions and not directly gathering patient information. When medical representatives exceed this authority by collecting detailed patient data, the processing often lacks a valid legal basis (eg, consent, legitimate interest or legal obligation). This exposes pharmaceutical companies to risks of non-compliance with potential legal liabilities.

Prescription Statistics for Commercial Purposes

In the current administrative regulatory framework, prohibitive provisions have been enacted against the practice of collecting prescription statistics for commercial purposes. These provisions specifically prohibit pharmaceutical companies or their employees from collecting prescription data of healthcare institutions, their internal departments or healthcare professionals.

Enforcement cases have revealed two typical illegal methods of obtaining prescription statistics for commercial purposes.

- The first involves bribing healthcare professionals with kickbacks in exchange for access to prescription data.
- The second is the unauthorised intrusion into the information systems of healthcare institutions to extract prescription-related information.

In recent years, subtler data collection practices that infer prescription statistics have emerged. These are often overlooked by pharmaceutical companies. For example, calculating patient counts using specific drugs under specific healthcare professionals, combined with dosage and administration data, can deduce prescription volumes. Another practice involves collecting institutional drug inventory data by cross-referencing distributor sales records (which companies typically hold) with inventory levels. This allows prescription volumes to be inferred.

Many pharmaceutical companies may implement data collection without realising these practices implicitly violate regulations, as they often frame inventory or patient volume tracking as routine operational analysis rather than unlawful prescription statistics. This lack of awareness increases legal risks, as regulatory scrutiny focuses on the nature of data use (regardless of intent) when the information can directly or indirectly reveal prescribing patterns.

Anti-Bribery and Anti-Corruption

The laws and regulations in the PRC have consistently imposed strict anti-commercial bribery and corrupt practices measures from both administrative and criminal perspectives. In recent years, the regulators' continuous efforts in targeting anti-bribery and anti-corruption in the healthcare sector have been seen.

In recent enforcement actions, there has been an increase in cases where pharmaceutical companies paying service fees to healthcare professionals through digital programmes such as patient education programmes and patient management programmes. Given that the healthcare professionals implicated did not perform substantive services and the payments offered by the companies exceeded the fair market value, the relevant authorities found these programmes involved irregularities in terms of commercial bribery and corruption.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com