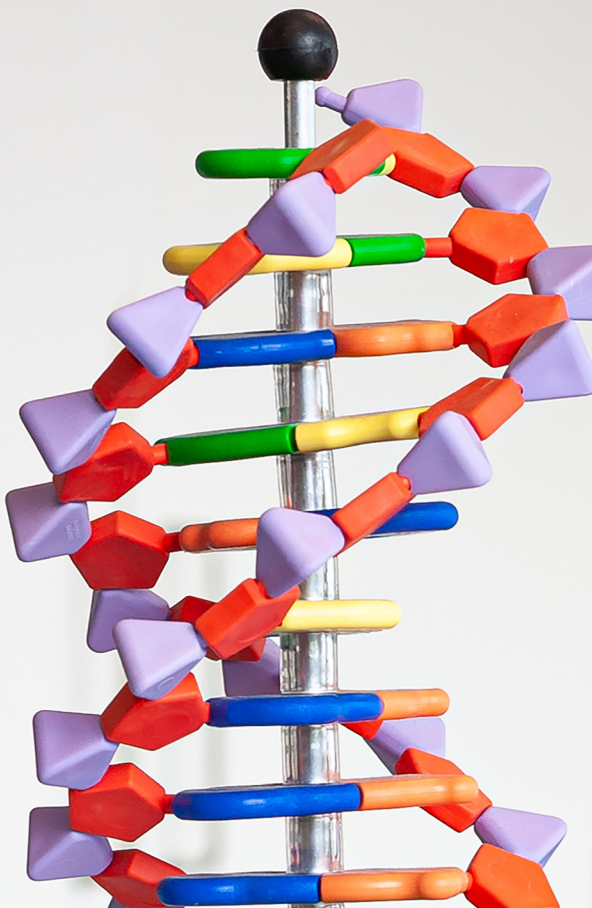
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Digital Healthcare 2023

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



China: Law & Practice

Alan Zhou, Charlene Huang, Jenny Chen and Sylvia Dong
Global Law Office

CHINA

Law and Practice

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

Contents

Global Law Office was one of the first law firms in the People's Republic of China (PRC), with more than 600 lawyers practising in its Beijing, Shanghai, Shenzhen and Chengdu offices. Its life sciences and healthcare (L&H) practice group, also known as China Life Sciences & Healthcare Law (CLHL), is one of the leading advisers in China, having provided "one-stop" legal services for every sector of the L&H industry, including R&D, clinical research organisations, pharmaceuticals, biotechnology, medical devices, supply producers and distributors, hospitals and other healthcare providers and investment funds. GLO 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, 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 head of life sciences and healthcare (L&H) practice of Global Law Office and the head of China Life Sciences & Healthcare Law (CLHL). He has been recognised as a pioneer in providing outstanding legal consulting services in the 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. He 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. He has won numerous awards and has been recognised by peers for his expertise, and 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 M&A 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 restructuring 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 the PRC, a certified fraud examiner of US ACFE, a certified public accountant (non-practising), and passed the US California Bar Exam. 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.

Sylvia Dong is an of counsel in Global Law Office based in Shanghai, an attorney at law in the PRC, and admitted to practice in New York State, USA. Her main practice covers M&A, PE/VC and capital markets, and she is especially focused on the life sciences industry and the TMT industry. She has rich experience in investment, licence deals, business collaborations, general corporate and compliance in the industry of life sciences and healthcare. She also represents well-known healthcare and telecommunications companies handling digital projects.

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

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Digital healthcare, digital medicine and digital therapeutics are not legal terms defined in People's Republic of China (PRC) laws and regulations, but are frequently referred to 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.

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

1.2 Regulatory Definition

As previously stated, digital healthcare, digital medicine and digital therapeutics are not legal terms defined in PRC laws and regulations, but are frequently referred to in commercial contexts and industry policies. Nevertheless, should any service or product in the fields of digital healthcare and digital medicine fall within the category of pharmaceuticals or medical devices, or be used for the diagnosis and treatment of human diseases, administrative regulations would correspondingly apply.

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
- the 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 used for assisted diagnosis and treatment, medical imaging, etc.

1.4 Emerging Legal Issues

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;
- PRC laws and regulations on cybersecurity and data protection; and
- PRC laws, regulations and industry standards on telecommunications and information technology.

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

Cybersecurity and Data Protection

As digital health involves a large amount of personal data, especially that of a sensitive nature, the design and implementation of life-cycle protection of such data needs to be carefully considered, under the cybersecurity and privacy protection laws and regulations – especially regulations of the PRC Personal Information Protection Law that came into effect on 1 November 2021.

Liability

As AI technologies are more frequently used in diagnosis and treatment by healthcare institutions, in circumstances where personal damages are caused to patients due to the application of such technologies, which party should assume responsibility 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, a series of notices and opinions were issued to encourage healthcare institutions to leverage telemedicine for the purpose of relieving the pressure on the offline delivery of healthcare services and ensuring COVID-19 patients' timely receipt of diagnosis and treatment.

2. Healthcare Regulatory Environment

2.1 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, and is responsible for their safety supervision and management, from registration and manufacturing to post-market risk management. Technology and devices, including software that falls within the category of a drug or medical device, are also subject to 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 and patients 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.

2.2 Recent Regulatory Developments

Regulatory Developments on Telemedicine

"Internet Plus Healthcare" – ie, healthcare in combination with application of the 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").

Furthermore, the NHC and the National Administration of Traditional Chinese Medicine released the Rules for the Regulation of Internet-based Diagnosis (for Trial Implementation).

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

In addition, the growth of internet-based diagnosis also boosted the demand for internet sales of medicine. Currently, with the Provisions for Supervision and Administration of Online Drug Sales newly enacted on 1 December 2022, except for medicinal products subject to special administration, internet sales of both over-the-counter drugs and prescription drugs are allowed.

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 prices and insurance policies to allow for internet-based healthcare services to be covered by China's medical insurance system. Implementation policies were further issued in 2020 and local enforcement rules have been gradually issued by local authorities since 2021.

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 cybersecurity 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, soft-

ware updates and related technical considerations. In 2021 and 2022 respectively, the NMPA issued the Guiding Principles for the Classification and Definition, and the Guiding Principles for Registration Review of AI Medical Devices, the latter laying out the application requirements and technical review standard of AI medical devices. In 2022, the NMPA issued a series of industry standards related to the quality requirements and evaluation of AI medical devices.

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 "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 mechanisms in digital medical insurance and digital healthcare.

From a general perspective, following two important data protection laws which took effect in 2021, the PRC Personal Information Protection Law and the PRC Data Security Law, a series of measures and guides related to data protection have been promulgated since 2022 regarding detailed regulations on data protection and security assessment measures for cross-border data transfer.

2.3 Regulatory Enforcement

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

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 involving sensitive information, including 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. 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.

In terms of internet-based diagnosis and treatment (including internet hospitals), as well as the basic Licence of Practice of the Medical Institution, issued by the NHC, medical institutions are also required to have the equipment, facilities, information system, technicians and information security systems that meet Level-3 information security protection, to be assessed by the PSB.

3. Non-healthcare Regulatory Agencies

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

The Cyberspace Administration of China

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

In terms of cybersecurity, the PSB 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.

Ministry for Industry and Information Technology

The MIIT is responsible for:

- regulating the information technology 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 related technology development, such as the development of and security requirements for AI technology. In addition, the MIIT actively leads personal data protection campaigns on mobile applications, including apps used in the healthcare industry.

New healthcare technologies have already prompted co-operation 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.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

Preventative care is not a legal term defined in PRC laws and regulations and can be interpreted broadly. In practice, if a preventative care concerns general healthcare consulting, elder care, nursery, massage, fitness or wellness, without making judgement about diseases or giving tar-

geted recommendations towards specific health issues or conditions, it may not fall within the definition of diagnosis and treatment and will not be subject to special regulation. On the other hand, if a preventative care falls within the area of diagnosis and treatment activities (eg, disease screening or vaccination), it can only be performed by a doctor qualified to practice in a medical institution.

4.2 Increased Preventative Healthcare

National polices have increased the awareness of preventative care. The State Council's Opinions for Implementing the Key Tasks Laid out in the Government Work Report of 2022 indicates that the State Council will adhere to the "prevention first" strategy in the "Healthy China Action" and strengthen health education and health management. The General Office of the CPC Central Committee and the General Office of the State Council's Opinion on Further Improving the Medical and Health Service System issued in March 2023 further stresses the ties between prevention and treatment of diseases, and requires relevant authorities to improve health promotion and preventative healthcare services for pregnant women, infants, students, occupational groups and the elderly. The government policies also focus on improving services, such as elder care, and supporting the revitalisation and development of traditional Chinese medicine (TCM), which will encourage awareness of preventative care.

Social trends also reveal the increased need for preventative care. On the one hand, as a result of the rapid development of the national economy and the expansion of the middle class, more consumers have begun to pursue a better quality of life and are willing to pay for preventative care. On the other hand, the outbreak of COVID-19 and the stress of the ageing population with limited social endowment insurance has also contributed to public health awareness.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Under PRC law, there is no clear separation of personal health data and fitness and wellness information. If certain fitness and wellness information also falls within the scope of personal information, information on human genetic resources (HGR) or healthcare big data, it will be regulated accordingly. The legal considerations can be reviewed in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information** and **11.1 The Utilisation of AI and Machine Learning in Digital Healthcare**.

4.4 Regulatory Developments

Currently, there are no detailed regulations focusing on preventative healthcare. However, national policies have been addressing this topic. For example, the 14th Five-Year Plan for the National Development of Undertakings on the Elderly and for the Elderly Service System stated that "preventative healthcare" for the elderly shall be strengthened, which is the prerequisite for developing elderly care services, combining medical treatment and elderly care. The Guiding Opinions on Promoting the High-Quality Development of Family Doctor Contracting Services issued by the NHC, NHSA, etc in March 2022 requires related regulatory authorities to facilitate the provision of public health services, including preventative healthcare, by family doctors. The Guiding Opinions on Further Promoting the Development of Integrated Medical and Nursing Care issued in July 2022 encourages commercial insurance coverage on preventative health care, health management, rehabilitation and nursing care for the elderly.

4.5 Challenges Created by the Role of Non-healthcare Companies

The healthcare industry is subject to relatively strict regulations in China. When a non-healthcare company enters the market by introducing new technologies and the application of existing technologies to healthcare, it must evaluate:

- whether the device using such technologies will be deemed as a medical device; and
- whether the application of such technologies will be deemed as provision of medical services.

In either case, entrants into the relevant market must first obtain a licence.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

Technology Developments Enabling the Enhanced Use of Connected Devices

Connected devices involve a wide range of technologies, including sensing technology, display technology and wireless communication technology. The development of endurance technology also enables the enhanced use of connected devices.

With the above-mentioned 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 to facilitate the provision of telemedicine services.

5.2 Legal Implications

If a telemedicine platform is aimed at providing health education or caring services rather than medical services, the user may claim for liability against the platform owner.

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

5.3 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. Taking reference from the Administrative Measures for Cybersecurity of Medical and Health Institutions and a series of policies, guidelines and recommended national standards, the healthcare institutions should:

- install and upgrade anti-virus software;
- detect Trojan viruses;
- monitor the access authority on open ports;
- manage the system; and
- carefully keep a system security diary.

Meanwhile, the healthcare institution should also:

- carry out daily information security monitoring and early warning checks;
- establish security incident reporting and response procedures; and
- formulate emergency response plans.

5.4 Proposed Regulatory Developments

A connected device intended for medical purposes is deemed to be a medical device and is subject to the regulations of the NMPA on medical devices.

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

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Definition and Regulatory Authorities

Under applicable PRC laws and regulations, standalone software as a medical device (SaMD) refers to software which has one or more medical uses, does not require medical device hardware to accomplish the intended use, and runs on a common computing platform. A 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, or in conjunction with specific medical device products based on a common, dedicated data interface.

As for a software product that uses AI, whether it is administrated as a SaMD depends on its intended use, processing object and core function, among other factors. When a software product processes medical device data and its core function is to handle, measure, model, calculate or analyse such data for medical purposes, the product falls within the scope of a SaMD.

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

Classification of a SaMD

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

- Class I is the 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 and image file transmission are classified as Class II devices, while most of the

SaMDs used for assisting treatment (eg, formulating a 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 the PRC and Class III medical devices must register with the NMPA.

Software updates of SaMDs can 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 SaMDs are subject to corresponding licensing requirements, in particular the Appendix for SaMDs of Good Manufacturing Practice for Medical Devices. In addition, the clinical use of certain 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 such technology.

7. Telehealth

7.1 Role of Telehealth in Healthcare

Internet Hospital

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

- offline healthcare institutions with their associated internet hospitals – eg, an internet hospital of a certain public hospital; and
- independent online hospitals set up with reliance on offline healthcare institutions – eg, an 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 on 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.

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, rehabilitation, smart-aided therapeutics, drug delivery and medication guidance services, etc. The residents can execute service agreements, make appointments, and accept health consultation and follow-up of chronic diseases 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 China made to patients located in China; though in practice the platform providing such services may be exposed to regulatory risks as physicians and nurses permitted to provide 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 diagnoses regulated by the Internet-based Diagnosis Measures.

7.2 Regulatory Environment

The NHC issued a series of notices and opinions in 2020 to encourage healthcare institutions to leverage telemedicine and release the pressure of offline delivery of healthcare services. Expanding the coverage of telemedicine and establishing a telemedicine collaboration network are also parts of the requirements to further improve the medical and health service system according to the General Office of the CPC Central Committee and the General Office of the State Council's opinions in March 2023. 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.

7.3 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 October 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 their internet-based diagnosis services via the BMI agencies. BMI reimbursement for internet-based diagnosis services may cover both medical consultation fees and drugs.

8. Internet of Medical Things

8.1 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 sensors, 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, 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 allows for more efficient and focused operations.

Wearable health monitoring devices

Wearable health monitoring devices refer to devices using wearable biosensors for collecting data on an individual's 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 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 upgrading 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 and wearable devices, 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.

9. 5G Networks

9.1 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 in high demand. A typical scenario is where 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 help to solve the issues of data sharing and cleaning to support the development and application of AI technologies. In this regard, from 2019 and led by the NHC, several sub-standards of Hospital Network Construction Standards Based on 5G Technology were compiled and released to guide the construction of a new generation of 5G network infrastructure of hospitals.

The Commercial and Contractual Considerations of Healthcare Institutions

Key commercial and contractual considerations faced by healthcare institutions in entering into arrangements with telecommunications providers to deploy and manage 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.

10. Data Use and Data Sharing

10.1 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 and the PRC Personal Information Protection Law 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 those involving public interest 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 a "limited data set", which means the data is subject to a certain degree of de-identification but may still identify the specific individual as 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 would then not be deemed as personal health data, but as general health data, subject to a relatively low level of protection. As for data aggregation, this 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 for obtaining consent. 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 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; and
- 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. For example, HGR, including HGR materials and HGR information, are not allowed to be shared with foreign parties without explicit approval or record-filing from the relevant authorities.
- Cross-border data transfer – whether the personal health data would fall within 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 a proper due diligence process has been completed on the capability of the transferee to ensure data security of the personal health data.

- Contractual agreement – whether a contractual agreement that stipulates the respective rights and obligations (including but not limited to security obligations of the transferee, scope of use by the transferee, restriction on sharing, retention period and disposal requirements, assumption of liabilities for data breach) has been concluded between the transferor and transferee.

Liabilities

As personal health data largely falls within the category of personal sensitive data under 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 for personal data, and are regulated under the PRC Criminal Law, the PRC Cybersecurity Law, the PRC Civil Code, and the PRC Personal Information Protection Law, which include criminal liabilities, administrative liabilities and civil liabilities as follows:

- criminal liabilities for infringement of personal data include criminal detention, a fixed-term sentence and monetary fines depending on the severity of the conduct and consequences;
- administrative liabilities for illegally processing personal data include 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 revocation of business licences under serious circumstances;
- personal liabilities imposed on the person in charge include fines of up to RMB1 million and prohibition from holding certain positions; and
- civil liabilities for infringement of personal data could be divided into tortious liabilities and liabilities for breach of contract.

11. AI and Machine Learning

11.1 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. From the legislative 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, pharmaceutical research, 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 include data security concerns, 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, the PRC Civil Code and the PRC Personal Information Protection Law.

Additionally, as a sizeable 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 back-up 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. As for the regulatory scheme, China is in the process of establishing laws and regulations, ethical norms and policy systems in AI development and application.

11.2 AI and Machine Learning Data Under Privacy Regulations

As addressed in **11.1 The Utilisation of AI and Machine Learning in Digital Healthcare**, companies engaging in new digital healthcare technologies should be aware of the relevant regulatory and legal issues, including cybersecurity and data protection, and that they are subject to the same requirements.

Unlike traditional medical devices, the development of an AI medical device may need a tremendous amount of data for machine learning and training. According to the national recommended standard on Information Security Technology – Guide for Health Data Security, the development and validation phase of a product where data relating to patients and related populations is required is essentially a clinical study. Collecting and processing personal information in a clinical study is also subject to the informed consent of the data subjects. In practice, as the digital companies may not need such data to be identifiable, they may choose to use a "limited data set" subject to a certain degree of de-identification which will not be deemed as personal information.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Licence to Practice

As addressed in **4.5 Challenges Created by the Role of Non-healthcare Companies**, new market players developing new digital healthcare technologies must first decide:

- whether the device will be deemed a medical device under PRC law; and
- whether the application of the device and/or the technologies will be deemed as providing a medical service.

In either case, entrants to the relevant market should first obtain a licence to operate and con-

tinuously follow the regulations of the healthcare industry.

In particular, due to the evolving nature of digital healthcare technology and the need for constant updates, any update of an algorithm due to increased amounts of data may require a change of registration of the medical device, which will need to be submitted to regulatory authorities for re-approval.

Cybersecurity and Data Protection

As addressed in **10. Data Use and Data Sharing** and **11. AI and Machine Learning**, companies engaging in new digital healthcare technologies should pay attention to the legal requirements for cybersecurity and data protection.

13. Upgrading IT Infrastructure

13.1 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; and
- elimination of information gaps among departments of the healthcare institution.

This would aim to achieve the goals of:

- resource sharing and business collaboration of healthcare services;
- supply of medical products;
- medical insurance; and
- comprehensive management.

From a cybersecurity and data protection perspective, 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.

13.2 Data Management and Regulatory Impact

In 2018, the NHC issued the Standards and Norms for Hospital Information Construction in China (Trial), which provides detailed requirements and standards for various levels of medical institutions with regard to software and hardware construction, security protection and application of emerging technologies, with IT upgrades as one of the requirements.

As for regulations on data management practices, other than the oversight of personal health information, as addressed in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**, patient information and other sensitive data should be stored within the PRC. A medical institution is required to enhance the informatisation level of clinical diagnosis and treatment and the use of electronic medical records, including:

- strengthening the protection of information systems;
- safe storage;
- disaster recovery and back-up of medical data; and
- prevention of information leakage.

14. Intellectual Property

14.1 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.

Patents

The PRC Patent Law protects inventions, utility models or designs that possess 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 a 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 the 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 a 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, commencing from the application date, are:

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

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 works.

Trade Secrets

Under PRC laws, trade secrets refer to commercial information such as technical information and business operation information not known to the public, that 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 a 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 an inventor of invention developed by AI has not yet been clarified under the PRC Patent Law. Currently, work generated with the 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 and with the company regarded as the author.

14.2 Advantages and Disadvantages of Protections

To decide which form of intellectual property protection applies to certain technology, the characteristics of the technology – ie, whether it satisfies the requisite elements of a specific form of intellectual property – need to be considered.

If the technology satisfies the features of more than one form of intellectual property, commonly between a patent and a trade secret, the technology owner needs to be aware of the advantages and disadvantages of different types of protection.

A patent right can be better claimed, proved and valued as it is reviewed and granted by the Patent Office and officially registered. Such protection is granted on the condition that the technology is reviewed, publicised and the protection duration is limited under the law.

Trade secret protections, on the other hand, require the owner to take relevant measures to keep such technology confidential and the protection does not have a time limit as long as the technology remains unknown to the public. However, in the case of a trade secret infringement, the owner will have to prove the existence of the trade secret, their rightful ownership, the occurrence of the infringement and its value.

14.3 Licensing Structures

The licensing arrangement of intellectual property could be different, depending on the commercial needs.

Provision of Services or Sale of Products

The provision of services or sale of products will not include a proprietary transfer of the intellectual property embedded in the services or products to the purchaser of the services or products. Similarly, the purchasers are not automatically granted a licence regarding the intellectual property except for the use of services or products they purchased for their intended use.

Licence Deal on Digital Healthcare Products or Technology

In a typical licence deal, the licensor will grant a licence to the licensee to develop, utilise, upgrade, improve and commercialise the digital healthcare products or technology. Such collaboration will generally include a licence of intellectual property rights and the consideration for such a licence, under which the licensee can use the intellectual property for agreed purposes and retain interest generated therefrom. Sometimes, the licensor will also ask for a right of grant-back to enjoy the improved technology and a right of

reference of the data generated from the licensee's use of the licensed products or technology.

Co-development

For digital healthcare services and products that are at an early stage of development, the parties may agree on a co-development of such technology or product and co-own the intellectual property rights derived therefrom.

14.4 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 that 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 materials 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 applications for work products generated from international co-operative research (eg, between a Chinese hospital and a foreign sponsor) utilising Chinese HGR, at least as regards clinical trials for non-registration purposes, such patent application should be submitted and the patent rights owned by both parties of the co-operation.

14.5 Contracts and Collaborative Developments

Where 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 on 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, licensing, transfer and profit distribution. 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.

15. Liability

15.1 Patient Care

Generally, with respect to the determination of liabilities in the event injury is incurred by a patient using a 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. Where 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 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 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, it shall also be held liable. The question of whether AI can conduct medical treatment independently and the related liability issues are to be further clarified by relevant laws and regulations.

In terms of the potential bias issue of AI, as bias would likely be deemed an ethical issue, this is to be further clarified by enforcement practice.

15.2 Commercial

Contractually, if the supply chain disruption or the cause thereof constitutes a breach of the agreement between the vendor and the healthcare institution, such as a failure of the vendor to perform certain obligations, 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.

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 Katie.Burrington@chambers.com