HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

November 4, 2016

Big Data Policy and Legal Issues in the Healthcare Industry

Min ZHU | Robin ZHANG

Introduction

With the continuous development of cloud computing and internet of things technology, the internet is further reshaping the healthcare industry. Informatization in hospitals is effectively advancing, and the mobile medical industry has also seen rapid development. The integration of internet technology and the healthcare industry has yielded an unprecedented expansion in the breadth of medical data. An increasing number of enterprises have begun to pay attention to big data mining and applications in the healthcare industry.

In light of these developments, on October 25, 2016, the CPC Central Committee and State Council jointly issued the "Healthy China 2030" blueprint (the **"Blueprint**"), to outline the action plan for the creation of a healthier China in the next 15 years. The Blueprint places particular emphasis on the development of the health industry, healthcare data and the nurturing of new applications for big data in the healthcare industry. Under State guidance and encouragement, healthcare big data has the potential to become a future impetus for growth in the healthcare industry. Further, the Blueprint also clearly proposes to strengthen the construction of laws and regulations and standards related to big data in the healthcare industry.

At present, the laws and regulations for healthcare big data have not kept pace with developments in this field. The development of big data in the healthcare industry has been seriously constrained by the lack of comprehensive guidance. Many private enterprises and foreign-funded enterprises have expressed a strong interest in healthcare big data, but market access and industrial policy uncertainties remain an obstacle. Market enthusiasm and vitality have thus not been fully and effectively released.

This article aims to analyze the potential policy and legal issues related to big data in the healthcare industry for reference and decision-making purposes.

The Concept of Big Data in the Healthcare Industry

As with “cloud computing” and the “internet of things,” big data is a new term that has been invented in recent years during this new phase of industrial revolution. According to the *Notice on Promoting the Development of Big Data,* issued by the State Council in August 2015, “big data” is a collection of data characterized by being of large capacity, of multiple types, and with fast access speed and high application value. Big data in the healthcare industry is classified as a subtype of big data and focuses on the integration and application of data in the healthcare industry.

The *Administrative Measures for Population Health Information (for Trial Implementation)* (“**Administrative Measures**”), promulgated in 2014 by the National Health and Family Planning Commission (“NHFPC”),defines “population health information” as personal health information, such as basic population information and medical treatment information generated from the provision of services and management by healthcare and family planning institutions at all levels and of all varieties in accordance with State laws, regulations and administrative duties. Thus, healthcare industry data mainly refers to personal immunization data, physical examination data, outpatient service data, hospitalization data and data related to other health activities. However, with the popularity of online smart devices, such as wearables, healthcare industry data may also include data generated by individuals using mobile healthcare applications.

The Value of Big Data in the Healthcare Industry and related National Macroeconomic Policies

Big data in the healthcare industry is a high value-added information asset. Although the individual healthcare data is insignificant to medical technology innovation, by collecting, storing, developing and studying the massive, scattered and diverse data, the healthcare services industry can discover new knowledge, create new value and enhance new capabilities. Therefore, the development of big data in healthcare industry has a stake in people's livelihood and is of great strategic significance.

To date, the central government has formulated relevant policies from time to time to support the development of big data in the healthcare industry, which has laid the basis for the development of big data in the healthcare industry.

a. NHFPC launched the "46312" project in 2014, which created a four level healthcare information platform (divided into national, provincial, prefectural and county levels)that supports six electronic health and medical record business applications: public health, medical services, medical insurance, drug management, family planning and integrated management. The platform consists of three databases, an electronic monitoring archives database, electronic medical records database and full population case database, establishes a single secure healthcare network, and strengthens the construction of the

health standards and safety standards systems.

b. In 2015, at the twelfth National People's Congress, Premier Li Keqiang proposed to formulate the "Internet +" action plan. The "Internet + Healthcare Industry" plan will further promote the integration of the internet and the traditional medical industry.

c. In June 2016, the General Office of the State Council promulgated the *Guiding Opinions on Promoting and Regulating the Application and Development of Big Data in Healthcare* (the "**Guiding Opinions**"), which pointed to the promotion of big data sharing in the healthcare industry.

d. On October 22, 2016, to promote and standardize the application of big data in the healthcare industry, Fujian Province, Jiangsu Province and the cities of Fuzhou, Xiamen, Nanjing and Changzhou were identified as the first group of pilot provinces and cities for establishing healthcare big datacenters and industrial parks.

e. On October 25, 2016, the CPC Central Committee and the State Council issued the Blueprint, which highlighted to strengthen the construction of application system of healthcare big data and promote the sharing, deep digging and extensive application of healthcare big data created based on regional population health information platform.

Practical Obstacles in the Development of Big data in Healthcare Industry

Although the central government encourages and supports the development of big data in the healthcare industry at the macroeconomic policy level, there continue to be a number of obstacles to overcome with respect to policy implementation, such as:

a. **Low Levels of Sharing and Openness with respect to Big Data in the Healthcare Industry**

Medical institutions are undoubtedly the main force in the collection and storage of healthcare big data. Compared to data derived from mobile healthcare applications, the data generated by medical institutions, particularly from electronic medical records (EMR), are more accurate and of a higher commercial development value. However, due to the data barriers that exist between medical and health institutions, and medical institutions and the public, it is difficult for medical institutions to share this data. Data isolation, on the one hand, results in the duplicate collection of patient data and waste of medical resources. On the other hand, it also hinders the systematic development of big data in the healthcare industry.

With the deepening of the reform of the medical system and the improvement of hospital informatization, the data barriers between medical institutions are expected to be further reduced. The Guiding Opinions require the establishment of a unified healthcare data sharing mechanism, with close cooperation across a broad range of administrative departments. The Blueprint seeks to eliminate data barriers and to establish close cooperation across

administrative departments and sectors to unify the sharing of healthcare data, so as to realize information system data collection applications, integration, sharing and business collaboration for public health, family planning, medical services, drug procurement, and integrated management.

Thus, with coordination across various departments under government leadership, the application of big data in the healthcare industry is expected to be developed in a systematic manner and data isolation is expected to be further weakened or even eliminated. However, it is yet unknown whether or to what extent these medical data resources will be open to private enterprises and foreign-funded enterprises. In addition, since the construction of the national medical data integration and sharing platform involves the efforts of multiple regulatory authorities and institutions, the coordination among these various bodies will be difficult in practice. To develop the platform would appear to require additional progress. Currently, private enterprises and foreign-funded enterprises are only permitted to access the data resources of medical institutions through bilateral cooperation. These business interests are carefully exploring the development and application of healthcare big data.

b. The Legal System related to Big Data in Healthcare Industry Requiring to be Improved

Healthcare Data Ownership: The current legal system does not clearly interpret or define the ownership of healthcare data, particularly with respect to the ownership of medical data. This issue has given rise to medical data ownership disputes between patients and medical institutions. Some believe that the since both the hospital and the patient are involved in generating medical data, the data should theoretically belong to both the hospital and the patient. Others argue that the ownership of medical data should belong to each individual patient, while hospitals should maintain control and the government should have administrative authority. In this case, third party institutions could develop and use of medical data with the cooperation of the government and the hospitals. This ambiguity with respect to the ownership of medical data restricts the authorized use of the data, and also poses a difficult problem for the protection of patient personal information rights.

Big data in the healthcare industry can be regarded as an information asset. Under the current legal system, if the medical institutions or authorized third parties legally process medical data so that it has intellectual property or economic value, the data may be protected as a type of intellectual property or trade secret. However, the original personal health information and data that medical institutions and mobile medical operators collect still falls within the scope of personal information and privacy, and can be protected from a personal rights perspective.

Legal Protection of Personal Data: Legislation with respect to the protection of personal information is under steady improvement. The draft *General Principles of Civil Law,* currently under consideration, is expected to separate personal information from privacy rights and will grant independent protection to personal information. As citizens increasingly perceive

personal information protection as a right, lawmakers are expected to speed up enacting and promulgating separate laws for personal information protection. The third review draft of the Network Security Law has been promulgated in October of this year and the final version is expected to be introduced at the end of this year or early next year.

It is noteworthy that, according to Article 41 of the Network Security Law, "network operators shall not disclose, tamper with or damage the personal information of citizens that they collect. Without the consent of citizens subject to information collection, such collected personal information shall not be provided to others, except for information that has been processed and cannot be identified or recovered". This provision provides that citizens' personal information must be anonymized before being used for big data applications. The handling and use of information therefore is not subject to personal information protection restrictions if the data collector can process the information so that the information of specific individuals cannot be identified or recovered. Legislators appear to have intentionally left a viable space in the system design for big data applications to achieve a balance between personal information protection and the public interest.

Legal Compliance Advice on the Development of Big Data in the Healthcare Industry

Although the development of medical data is encouraged at the macro-policy level, there are still no systematic or detailed rules related to big data in the healthcare industry. Nevertheless, based on our observations of industry practice and in light of current legislative trends, we have summarized the following legal compliance recommendations for your reference:

a. **Standardizing Data Collection in the Healthcare Industry**: (i) Entities collecting medical data through self- or affiliate-developed platforms are required to act in accordance with the principles of lawfulness, reasonableness and necessity. The collecting entities should expressly indicate the purpose, manner and scope of collection and use of the personal information collected through a privacy policy or by other means and obtain consent of the individuals whose information is being collected or used; (ii) If the entity relies upon sharing medical data with medical and health institutions, the entity should set up patient data protection firewalls and anonymize the collected information so that specific individuals' information cannot be identified and recovered.

It is noteworthy that the European Union has promulgated the *General Data Protection Regulation* (the "**Regulation**") in April 2016, which is regarded as the most stringent data protection regulation in history. The Regulation sets forth the principles of transparency and data minimization for the processing of personal data and grants to individual data collection subjects the right to withdraw consent, the right to erasure and the right to portability.

Although these principles have not yet been clearly defined in PRC law, as the legislative process for the protection of personal information and the progress of economic globalization

deepen, it is believed that China will draw lessons from the experience of developed countries with respect to personal information legislation. Therefore, we recommend that multinational companies which are subject to higher compliance standards consider the relevant provisions of the Regulation in practice.

b. **Local Storage and Overseas Data Transmission**: with the current emphasis on cyberspace sovereignty, entities must store medical data within territory of China and must not transmit sensitive medical data overseas if it is uncertain whether such outbound transmission will damage State security, people's livelihoods or the public interest.

At present, there is no law forbidding the extraterritorial transmission of big data or personal information in the healthcare industry. The draft *Anti-Terrorism Law*s ought to require telecom and internet service providers to keep the relevant equipment and domestic user data within China. However, the provision provoked great controversy and was ultimately struck from the officially promulgated version of the law, dated December 27, 2015. It should be noted that the Network Security Law (second draft for review) has introduced the concept of "critical information infrastructure" and provides that the operators of critical information infrastructure cannot transmit abroad citizens' personal information and important business data that is collected and stored during operations. In this sense, if the medical data processing platform is regarded as critical information infrastructure, exporting citizens' personal information collected and stored on the platform will be subject to the appropriate safety assessment. Even if such data is free of personally identifiable information, it could still fall into the category of "important business data", which would also subject the export of such information to strict restrictions.

At the regulatory level, the Administrative Measures explicitly prohibit the storage of population health information on offshore servers. However, strictly speaking, this restriction is only limited to personal health information, basic population information and health information generated by various medical, health and family planning services institutions. Thus, this provision does not apply to general personal health information collected based on mobile healthcare applications or anonymized population health information data.

i. **Improve Security Measures**: Medical big data platform operators should undertake technical and other necessary measures to ensure information security and prevent damage to, or the leak or loss of personal information collected during business operations. Operators should immediately perform remedial measures in the case of actual or possible damage to, or the leak or loss of collected personal information. In addition, operators should undertake data security measures that meet the appropriate standards. The Network Security Law (second draft for review) stipulates that the government will implement a hierarchical network security protection system. Network operators should establish an internal compliance system to fulfill the security protection obligations for the corresponding security grade.

The Network Security Law is in fact not the first law to require the establishment of security grading protection system. According to Article 7 of the *Administrative Measures for Hierarchical Protection of Information Security (*the "**Protection Measures**"*)* jointly promulgated by the Ministry of Public Security, the State Secrets Bureau, the State Cryptography Administration and the Information Office of State Council in 2007, the information security protection system is divided into five grades. Information system operators and users are required to protect information security in accordance with the *Guidance on the Implementation of the Hierarchical Information Security Protection System*. Further, after completion of the information system, operators and users, or the competent authority, will select an evaluation institution that meets the conditions stipulated in the Protection Measures to carry out a rating assessment of the information system security grade status on a regular basis according to the technical standards stipulated in the *Assessment Requirements for the Hierarchical Information Security Protection System* and carry out filings as required.

Further, the *Guiding Opinions on Hierarchical Security Protection Work in the Healthcare Industry,* promulgated by the Ministry of Health in 2011, categorize information security protection into five grades: 1)autonomous protection, 2) directed protection, 3)supervised protection, 4)mandatory protection, 5)special control protection. In principle, the security protection over important medical information system is at or above the third grade.

Since medical big data platform information processing and the resulting applications for that information mainly involve the healthcare industry, it is recommended for operators in this field to establish and implement a hierarchical data security protection system according to the provisions and standards stipulated in the *Guiding Opinions on Hierarchical Security Protection Work in the Healthcare Industry*.

ii. **Restrictions on Foreign Investment related to Big Data in the Healthcare Industry**: Although there are no regulations directly restricting or prohibiting the participation of foreign capital in the field of medical big data, the collection and processing of data that involves human genetic resources is subject to the *Interim Measures for the Management of Human Genetic Resources* (1998) and the *Service Guide on the Administrative Licensing Items concerning Collection, Collection, Sale, Export and Exit Licensing of Human Genetic Resources* (2015). Collecting human genetic resources in cooperation with foreign parties or enterprises with foreign investment or transmitting human genetic resources overseas can be conducted only after approval from the Ministry of Science and Technology.

Foreign investment in medical big data may also be restricted with respect to the operating mode and specific business structure of the medical big data platform. For example, if a multinational company intends to set up a medical big data platform through establishing a specialized medical institution, the multinational would be subject to restrictive foreign investment policies related to medical institutions. If the multinational plans to process medical big data through a cloud platform, networking platform or block chain-based technology BaaS

platform, it may be subject to foreign investment restrictions in the field of value-added telecommunications. In addition, cooperation between multinationals and medical institutions may also be impeded by medical institutions' hidden preference for domestic investors.

In summary, it is not presently possible to generalize with respect to foreign investment restrictions facing the development of and applications for medical big data platforms in China. In practice, an analysis must be conducted based upon the scope of the data involved, the operating mode and the specific business structure of each data platform.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact **Min ZHU (+8621-60800955; min.zhu@hankunlaw.com）.**