漢坤律師事務所
HAN KUN LAW OFFICES

Newsletter

11th Edition of 2016

Legal Updates

1. Comments on the Network Security Law
2. Big Data Policy and Legal Issues in the Healthcare Industry

Legal Updates

1. Comments on the Network Security Law (Authors: David TANG, Robin ZHANG, Effy SUN)

On November 7, 2016, the *Network Security Law of the People's Republic of China* (the "**Network Security Law**") was adopted at the twenty-fourth meeting of the 12th National People's Congress after the third draft. The Network Security Law is composed of 7 chapters and 79 articles and will come into effect on June 1, 2017.

The Network Security Law will apply to the construction, operation, maintenance and use of networks as well as the supervision and administration of network security within the territory of the People's Republic of China (hereinafter, "**China**"). Below, we review and summarize some important systems and highlights of the Network Security Law.

Emphasizing national sovereignty and security in cyberspace

With the development of Internet and information technology, national sovereignty in cyberspace is facing significant challenges. The worldwide network environment may appear calm on the surface, but significant risks are present underneath. Network security is becoming a major issue of national sovereignty, security and interest. In response, many countries around the world have been formulating legal measures and building monitoring systems to maintain network security.

Take the European Union, for example. The European Court of Justice, the highest judicial body of the European Union, entered a judgment in October, 2015 that invalidated the safe harbor agreement regarding automatic data exchange, which was signed between the European Union and the United States in 2000. In April, 2016, the *General Data Protection Regulation* was adopted by the European Parliament after four years of discussion and has been regarded as the most stringent regulation for personal data protection. In July, 2016, the European Parliament adopted the *Instructions of Network and Information Security,* which marked the first network security act formally issued by the European Union.

Against this backdrop, China has passed the new *National Security Law* in July, 2015 and has defined the concept of "national cyberspace sovereignty". The *Outline of National Informatization Development Strategy*, promulgated in July, 2016, underscores the safeguarding of national sovereignty, security and development interests in advancing the promotion of national informatization construction, as well as accelerating network security legislation.

The Network Security Law follows the State's holistic development approach, and applies equal weight to network security and informatization. The Network Security Law also puts into practice relevant rules and measures for the protection of key information infrastructure, network information security, monitoring, early-warning and emergency responses, and legal liability. In particular, the

final draft of the Network Security Law adds accountability measures for non-PRC persons.[1] These measures enhance defense and deterrence with respect to network sovereignty.

Implementing a hierarchical network security protection system

The Network Security Law requires a hierarchical network security protection system,[2] but this system was not first proposed by the Network Security Law.

In 2007, *Administrative Measures for Hierarchical Protection of Information Security* was promulgated by Ministry of Public Security, State Secrecy Bureau, State Encryption Administration and the Information Office of the State Council. Article 7 of the Administrative Measures divides the information security protection system hierarchy into 5 grades, and entities operating or using information systems are required to take concrete measures to carry out protection pursuant to *the Guidelines for Implementing the Hierarchical Information Security Protection System*. After the construction of an information system is completed, the entity operating or using the information system, or the competent department, will select a testing and evaluation agency that satisfies the conditions according to the Administrative Measures to regularly test and evaluate the security of the information system pursuant to the *Requirements for Testing and Evaluating the Hierarchical Information Protection Security System* and other relevant technical standards, and go through record-filing procedures.

Based on the *Administrative Measures for Hierarchical Protection of Information Security* in 2007, the relevant competent authorities have further promulgated guidelines and standards to enhance information security in their respective fields. For example, the November, 2009, *Notice of the General Office of Ministry of Education on Carrying out Hierarchical Protection for Information System Security* requires college, university, and certain education department information systems of Grade III or above to undergo record-filing with the Education Management Information Centre of the Ministry of Education and local public security departments. The November, 2011, *Guiding Opinions of the Ministry of Health on Hierarchical Protection of Information System Security in the Healthcare Industry* requires information systems of Grade II or above to undergo record-filing with public security departments and health administration departments. Consequently, once the information systems of entities in certain industries reach a specified security grade, these entities will be supervised by both the public security departments and the competent departments in charge of that industry.

Furthermore, the *Administrative Measures for the Security Protection of Communication Networks*, promulgated by the Ministry of Industry and Information Technology in January, 2010, requires telecommunications operators and internet domain name service providers within China to partition

[1] Network Security Law, Art. 75. Non-PRC persons are subject to legal liability for activities that endanger key information infrastructure within the territory of the People's Republic of China, including attacks, intrusions, interference and damage that cause grave consequences. The Ministry of Public Security and relevant departments of the State Council have the right to freeze assets or impose other necessary punishment measures upon such non-PRC institutions, organizations and individuals.

[2] Network Security Law, Art. 21.

their officially operating communications networks and to classify their networks into five grades based upon the degree of potential damage to national security, economic function, social order and public interest. Such persons are also required to perform the relevant filing procedures with the telecommunications administration authorities, implement security protection measures and conduct compliance tests.

As China's first specialized cybersecurity law, the Network Security Law legally requires national implementation of the hierarchical network security protection system for the first time,[3] although specific mechanisms and standards have not been formulated. It is therefore presently unclear whether operators must follow the dual-track supervision mode under the authority of the public security departments and assisted by the competent departments in charge of industry, or whether a unified network security classification scheme will be formulated in the future. This issue will require further monitoring.

Carrying out important protection of key information infrastructure

The Network Security Law introduces the concept of "key information infrastructure" and carries out important protections on the basis of a hierarchical network security protection system as described above. As a strategic resource to national security and interests, the importance of key information infrastructure cannot be overstated. The importance of protecting key information infrastructure in law and policy has become a legislative trend for many countries around the world.

The definition of key information infrastructure was subject to significant revisions from the first draft to the third draft of the Network Security Law. The final draft provides an open-ended definition, which contains many important industries and fields, including public communications and information services, energy, transportation, water conservation, finance, public services and e-government, and relevant key information infrastructure that could endanger national security, people's livelihoods and the public interest in the case of damage, loss of function or data leakage. The detailed scope of and security protection measures for key information infrastructure is to be formulated by the State Council. The definition roughly describes the attributes associated with key information infrastructure through listing these sectors. On the other hand, the definition leaves flexibility for the State Council to further determine the specific scope and to formulate security protection measures.

The Network Security Law mainly undertakes important key information infrastructure protection measures as follows:

a. Article 35 stipulates that operators of key information infrastructure that purchase network products and services which could affect national security must pass a security review organized

[3] Network Security Law, Art. 21.

by the national Internet information department in conjunction with the relevant departments of the State Council. At the same time, the Network Security Law provides for corresponding punishment in the legal liability chapter.[4]

It is worth noting that the national security review of key information infrastructure was not first proposed by the Network Security Law. The *Foreign Investment Law of the People's Republic of China (Draft for Comment),*[5] promulgated in early 2015, lists the impact on key infrastructure and technologies as a factor to be considered during the national security review for proposed foreign investments. Thus, we can perceive and appreciate the strategic significance of key (information) infrastructure to the national security.

b. Article 37 establishes the relevant principles for cross-border information transmission for key information infrastructure, namely that personal information and important data collected and generated in the operation of key information infrastructure operators within China must be stored domestically. Where it is necessary to provide such information and data overseas due to business needs, a security assessment is required to be carried out according to measures formulated by the national Internet Information Department in conjunction with the relevant departments of the State Council, absent any contrary legal or regulatory provisions.

   So far, the Network Security Law is the first law to restrict the transfer of data overseas. However, this restriction only refers to personal information and important data collected and generated by the operation of key information infrastructure operators within China. Notably, the information scope of restricting the transfer of data was "personal information" and "important business data" in the second draft, but has been broadened to "important data" in the final draft, thus widening the scope of the transfer restriction.

Improving Personal Information Protection

a. Expanding the Scope of Protected Subjects: Compared to the previously issued second draft, the Network Security Law removes the restriction on "personal information" to be of "citizens", which broadens the scope of protected subjects to include all individuals using PRC network services, whether domestic or overseas. The aim is to avoid a legislative vacuum with respect to protecting the personal information of non-citizens.

b. Definition of Personal Information: Article 76 of the Network Security Law provides that personal information refers to all kinds of information, recorded electronically or otherwise, that can identify, independently or in combination with other information, a natural person's personal identity information, including but not limited to the natural person's name, date of birth, identification number, personal biometric information, address, telephone number, etc. This definition,

4 Network Security Law, Art. 66.

5 Foreign Investment Law of the People's Republic of China (Draft for Comment), Ch. 4.

although relatively broad, does not include information that can identify, independently or in combination with other information, when and where the user used the service,[6] which contrasts with the *Provisions on the Protection of Personal Information of Telecommunications and Internet Users* enacted in 2013.

c. Development and Application of Big Data: Article 42 of the Network Security Law prohibits network operators from divulging, distorting or damaging personal information that is collected, and from providing personal information to others without the consent of the person whose data has been collected, except where the information has been irreversibly anonymized. This exception would appear to free network operators from personal information protection rules when using such legally collected data if it has been processed so that specific individuals are unidentifiable and their identities are unrecoverable. This reflects legislators' intent to create feasibility for big data applications at the legislative level, so as to strike a balance between protection of personal information and the public interest.

d. Imposing Information Security Obligations on Network Operators: The Network Security Law consolidates the current provisions applicable to the protection of network information, such as the *Provisions on Protection of Personal Information of Telecommunications and Internet Users*, the *Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection*, the *Administrative Measures for Online Trading*, the *Law on the Protection of Consumer Rights and Interests*, the *Several Provisions on Regulation of the Order of the Internet Information Service Market*. Such provisions require network operators to, among others: disclose their rules for data collection and use, collect and use information as agreed, provide for certain safeguards to ensure information security and prevent information from being compromised or lost, and promptly undertake remedial measures when any information is or may have been compromised or lost. Any individual that discovers the illegal collection or use of personal information by a network operator can require the network operator to take remedial measures, and the network operator is explicitly required to take such measures.[7]

   Article 49 of the Network Security Law stipulates that network operators should cooperate with the lawful monitoring and inspections by the Cyberspace Administration and relevant authorities. This provision, however, does not articulate the extent of such cooperation and due process of the authorities, which may result in controversies or even the abuse of power during monitoring or inspections.

e. Punishment for Illegal Acts such as Online Fraud: Article 46 of the Network Security Law provides that individuals and organizations will be held responsible for their use of networks, and cannot set up websites or communication groups for the purpose of committing fraud, imparting criminal

6 Provisions on Protecting Personal Information of Telecommunications and Internet Users, Art. 4.

7 Network Security Law, Arts. 40 to 45.

methods, manufacturing or selling prohibited goods, nor publish information online regarding such illegal activities. The regulatory authorities may impose punishment on such violators in accordance with Article 67. This article was not contained in the second draft, but appears in the officially promulgated Network Security Law, and reflects legislative and regulatory bodies' determination to regulate the currently flourishing telecommunications fraud and e-commerce disorder.

Liabilities

The Network Security Law amends some of the punishment standards compared to the second draft, such as doubling the monetary penalties for certain illegal acts. Different industry access bans apply to acts that prejudice network security, which include unlawful intrusion into the networks of others, interference with the functioning of the networks of others, theft of network data, or the provision of services for such activities. Persons subject to public security administration punishment cannot take key positions in network security administration and network operations for five years, and criminal violators are subject to a lifetime ban on taking such positions.[8]

Summary of Other Highlights

a. Attention to Juvenile Protection: Article 13 of the Network Security Law calls for research and development of network products and services beneficial to the health of minors, and punishes activities harming physical and mental health of minors through networks with specific punishments. The aim is to provide for a secure and healthy network environment for minors.

b. Definition of "Network Operator": Article 76 of the Network Security Law defines "network operators" broadly to include network owners, administrators and service providers, which basically includes all types of persons that carry out activities through networks. The Network Security Law may therefore apply to any for-profit or non-profit entity that provides network services or provides products and services in China via communications networks, the Internet, etc.

c. Real-Name Verification: Article 24 of the Network Security Law requires real-name verification. Network operators must require users to provide genuine identity information when entering into agreements or confirming the provision of services regarding network access, domain registration, landline or mobile telephone network access, information publication or instant communication services. Relevant network service providers and network operators are required to strictly abide by these regulations and standards.

d. Regulatory Authority Confidentiality and Compliance Obligations: Given that regulatory authorities will receive large amounts of information during routine regulatory activities as well as

8 Network Security Law, Art. 63.

during the investigation and punishment of illegal acts, Article 30 of the Network Security Law provides that the relevant authorities may only use information obtained when executing network security protection duties as is necessary for maintaining network security.

In addition, Article 14 of the Network Security Law, concerning the reporting of illegal acts, requires the relevant authorities to keep confidential the informant's information and to protect his or her lawful rights and interests. This also encourages positive reporting and facilitates public supervision.

e. Monitoring, Precautions and Emergency Management: Network security is to be maintained through advance precautions, prevention during the course and post-event management. The Network Security Law requires network operators to establish contingency plans in case of network security events.[9] In addition, Chapter 5 of the Network Security Law specifically provides for the establishment of network security monitoring, precautions and emergency treatment, requires the setting up of network security monitoring, precautions and information reporting systems at the national level. These requirements are intended to enhance network security event risk prevention mechanisms and to promote network security event treatment mechanisms, while also introducing relevant laws and regulations including the *Emergency Response Law of the People's Republic of China* and the *Work Safety Law of the People's Republic of China*.[10]

Recap and Commentary

The Network Security Law, the first specialized cybersecurity law in China, concisely consolidates into a single law the provisions on network security and information protection contained in various lower-level laws. The law also marks a milestone by addressing the evolution of big data and informatization. A major reason for network security events and information leaks that have occurred in China in the past has been the absence of legislation and slack enforcement. Insignificant costs associated with violations and light punishment cannot act to draw enough attention to online information protection, nor encourage network operators to take sufficient protection measures.

In recent years, the PRC government has paid increasing attention to regulating network security and protecting personal information. Therefore, all domestic enterprises, whether network owners, administrators, or the vast number of network product and service providers, should strictly comply with requirements of the Network Security Law and carefully implement network security and personal information protection measures. At the same time, the Network Security Law will still need to be improved through experience from practice, as well as through promulgating supporting laws, regulations, administrative measures and standards. We will continue to monitor subsequent

9 Network Security Law, Art. 25.

10 Network Security Law, Ch. 5.

developments related to the Network Security Law.

==========

2. Big Data Policy and Legal Issues in the Healthcare Industry (Authors: Min ZHU, Robin ZHANG)

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 Newsletter 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 This Newsletter 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:

Contact Us

Beijing Office
Tel.: +86-10-8525 5500
9/F, Office Tower C1, Oriental Plaza
No. 1 East Chang An Ave.
Beijing 100738, P. R. China

Estella CHEN Attorney-at-law
Tel.: +86-10-8525 5541
Email: estella.chen@hankunlaw.com

Shanghai Office
Tel.: +86-21-6080 0909
Suite 5709, Tower 1, Plaza 66, 1266 Nanjing West Road,
Shanghai 200040, P. R. China

Yinshi CAO Attorney-at-law
Tel.: +86-21-6080 0980
Email: yinshi.cao@hankunlaw.com

Shenzhen Office
Tel.: +86-755-3680 6500
Room 2103, 21/F, Kerry Plaza Tower 3, 1-1 Zhongxinsi Road, Futian District, Shenzhen
518048, Guangdong, P. R. China

Jason WANG Attorney at-law
Tel.: +86-755-3680 6518
Email: jason.wang@hankunlaw.com

Hong Kong Office
Tel.: +00852-2820 5600
Suite Rooms 2001-02, 20/F, Hutchison House, 10 Harcourt Road, Central,
Hong Kong, P. R. China

Dafei CHEN Attorney at-law
Tel.: +852-2820 5616
Email: dafei.chen@hankunlaw.com