KANTAR

BIG DATA IN CHINA

Managing Regulatory and Compliance Issues

by Dr. Jessica Santos

Healthcare industry stakeholders are aware that China presents tremendous growth opportunities for healthcare therapies due to its immense size and scope, increased affluence, and growing appetite for innovative treatments. However, successfully conducting business in this dominant market requires effective management of regulatory and compliance issues for Big Data and data privacy. In this paper, we'll examine key factors to watch out for as you plan or update your business strategy for the Chinese market. These include:

1. China's New Cybersecurity Law
2. Real-World Evidence for Drug Discovery and Development
3. The Types of Healthcare Data that are Regulated in China
4. Regulations on the Management of Human Genetic Resources (HGRs)
5. Key Takeaways

© 2019 Kantar

1. Cybersecurity Law

China's new Cybersecurity Law, which was adopted by the National People's Congress in 2016 and came into effect in June of 2017, regulates the collection and use of personal information and important data in China. The law defines personal information as various information that's recorded by electronic or other means that can identify the natural person's personal identity alone or in combination with other information. This includes but is not limited to the name of the natural person, date of birth, ID number, personal biometric information, address and phone number. Companies aiming to do business in China should extend their focus from purely "data security" to the protection of personal information and privacy, as well as data with a broader scope of influence.

THE BASICS OF THE LAW

Network Operators

The Cybersecurity Law defines several security responsibilities for "network operators". The network operator is the owner, administrator and/or network service provider of the network. Network operators may provide network access and domain registration services for users; handle network access formalities for fixed-line or mobile phone users; provide users with information publication services, instant messaging services and other services; and may require users to provide identity information (instead of pseudonym) when signing agreements with users or confirming the provision of services. Most large financial institutions. research agencies and any other entities that host and collect personal information may be classified as network operators.

Critical Information Infrastructure

Protection requirements for "critical information infrastructure" are repeatedly detailed in the Cybersecurity Law. These include stringent requirements for the protection of critical information infrastructure, such as sensitive information preservation, where the Cybersecurity Law requires that important security data collected or generated by domestic operations be stored in the territory. Also, with regards to product safety, the law states that network-critical equipment and network security-specific products shall only be sold or provided after passing a safety certification.

Additionally, the Cybersecurity Law requires that sensitive data be stored locally. This directive includes restrictions on the transmission of personal and business data to overseas entities. These restrictions are highly relevant because foreign companies and organizations usually need to transmit data overseas.

Penalties

Multi-national corporations (MNCs) face significant legal liabilities for violating China's Cybersecurity Law. Clear penalties, including the suspension of business activities and the revocation of licenses, can be imposed on enterprises and organizations for serious violations of the law, with financial penalties reaching as high as RMB 1 million. There were 15 enforcement cases in the first three months alone, including orders of rectification, cease of data processing, and fines of up to a half million RMB.

© 2019 Kantar

KEY ARTICLES

The Cybersecurity Law applies to both personal information collection and protection, as well as the storage of sensitive information and overseas transmission of data.

Personal Information Collection and Protection:

Network operators that collect and use personal information have immense responsibilities.

For example, they should follow the principles of legality, propriety, and necessity (Article 41); handle the personal information it holds in accordance with the provisions of laws, administrative regulations and agreements with users (Article 41); must not disclose, tamper with, or damage the personal information they collect (Article 42); and providers of network products and services that collect user information should clearly obtain consent from users (Article 22).

Furthermore, departments responsible for cybersecurity supervision and management, in accordance with the law, must strictly keep confidential the personal information, privacy and business secrets that are known in the performance of their duties (Article 45). And, no individual or organization may steal or otherwise obtain personal information (Article 44). If individuals find that network operators violate the law, they have the right to ask network operators to delete their personal information (Article 43).

Sensitive Information Storage and Overseas Data Transmission:

Personal information and important data collected shall be stored in the territory if its generated by operators of key information infrastructures operating within the territory of the People's Republic of China. If it's necessary to provide overseas services due to business needs, operators shall conduct safety assessments in accordance with the methods formulated by the State Administration of Credit and the relevant departments of the State Council (Article 37).

For enterprises that need to transfer data to headquarters, partners and/or suppliers located outside of the country, they'll need to meet the conditions of the "critical information infrastructure" operators and their content and methods of transmitting data to the outside world will need to be evaluated. For personal information and important data stored outside of the country, the most direct and effective way to comply is to transfer the relevant data to domestic storage.

It's worth noting that most countries have restrictions on international data transfer in their national privacy legislations. However, the Chinese requirement certainly put more liability on the sender than receiver compared with other legislations, for example GDPR, CCPA, and PIPA.

© 2019 Kantar

2. Real World Evidence

Real-world evidence (RWE) supports both medicine discovery and development. The State Council of China encourages research and the creation of new drugs, and promotes the technical standards for drug registration to be in line with international standards.

To use RWE to support drug discovery, it's first necessary to clarify the definitions of real-world research. By identifying real-world research-related definitions, we can avoid some common misunderstandings, such as erroneously equating observational research with real-world research, real-world data analysis, research results, RWE, and traditional Randomized Clinical Trials (RCT). We also can avoid limiting the real-world research, which is of great significance for the rational selection of data sources and research types to support drug development.

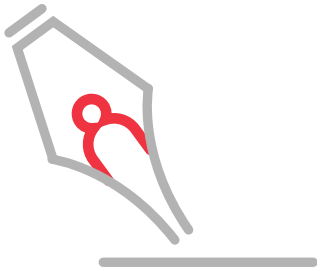
It's also necessary to conduct a source and quality evaluation of real-world data. This guideline provides a brief introduction to the potential sources of real-world data in the country, including but not limited to health information systems, healthcare systems, disease registration systems, and prospective research designs that actively collect data reflecting patient medication and health status. It also provides a view to selecting real-world data development ideas during research and development. Moreover, the quality of real-world data is primarily assessed through its relevance and reliability.

RWE can support drug development in a variety of ways, and its potential uses include pre-marketing clinical development and post-marketing re-evaluation. This guideline lists several scenarios that support drug development and regulatory decision-making, and several cases in which Chinese regulators make decisions based on RWE. It's worth mentioning that some drugs are widely used in clinics but have not been approved for marketing, especially with regards to traditional Chinese medicine. This is unique to China.

The basic design of real-world research includes practical clinical trials, one-arm trials and observational studies using real-world data as controls. It's noteworthy that real-world research design does not mean that it is mutually exclusive with random quality control measures. The research design that should be selected should be combined with specific research and development purposes. In contrast to RCT studies, causal inference in real-world research requires special attention to the adjustment of confounding effects, so some relatively complex statistical models and analytical methods are used.

Finally, there are two main principles for evaluating RWE– whether the RWE can support scientific questions that need to be answered, and whether existing real-world data can be scientifically analyzed to obtain the required RWE.

© 2019 Kantar



3. Types of Healthcare Data Regulated in China

According to the National Law Review, healthcare data can come from various sources, including medical record information, medical insurance information, healthcare logs, human genetic resources (HGRs), medical experiments and scientific data. These sources all have unique benefits and contribute greatly to medical advancement, but have different regulatory compliances factors and may have some overlap.

TYPES OF HEALTHCARE DATA REGULATED IN CHINA

Healthcare Big Data

This healthcare data is generated in the course of disease prevention, treatment and control, as well as health management. Key regulatory and compliance issues concern localization and storage, and security assessments for the cross-border transfer of data.

HGRs

HGRs data is genetic materials and related information, including organs, tissues, cells, blood, preparations, and recombinant deoxyribonucleic acid (DNA) constructs containing human genome, genes and their products. Key regulatory and compliance issues concern collection, as complex approval procedures are required and collection by foreign entities or individuals is restricted. Localization and storage regulations are also in play, as well as the need for approval from administrative bodies before cross-border transfers.

Pharmaceutical Data

Pharmaceutical data pertains to data from all activities in a product's life cycle, such as R&D, production, circulation, post-marketing monitoring and evaluation. Key regulatory and compliance issues concern laws and regulations on personal information protection, healthcare Big Data protection and human genetic information protection, which may apply under certain circumstances.

Medical Device Data

Medical device data pertains to healthcare data and device data. Key regulatory and compliance issues concern legislation on personal information protection, healthcare Big Data protection and human genetic information protection, which may apply under certain circumstances.

Medical Records

Medical records involve all texts, symbols, graphics, images and slides produced in medical activities by medical personnel. These include outpatient (emergency) records and hospitalization medical records. Medical records are filed as medical history. Key regulatory and compliance issues concern collection, as consent from data subject is required, as well as transfer, whereas medical institutions should keep records strictly confidential except under specific circumstances.

Scientific Data

Scientific data is primarily data that's produced from basic research, application research, pilot development and other endeavours in areas such as natural science and engineering technology science. It's also original data and data derived via observation and monitoring, survey and investigation, and inspection and detection that's used for scientific research activities. Key regulatory and compliance issues concern data transfer, especially data involving state secrets, which is strictly forbidden for third party transfers.

© 2019 Kantar

4. Regulations on the Management of HGRs

China's State Council, the country's top administrative authority, released a new regulation of Human Genetic Resources (HGR) on May 28, 2019, regarding it as a national security priority. The regulation covers the collection, storage, exploitation and sharing of HGRs, and requires that Chinese entities must notify the HGR regulator when disclosing or sharing any HGR-derived data to foreign-owned entities.

The regulation scrutinizes all HGR-related activity – from the upstream collection of human biospecimens, to the downstream exploitation and sharing of the material and any data obtained from it. It also formalizes the approval requirements pertinent to research collaborations between Chinese and foreign-owned (including both partially and wholly foreign-owned) entities to avoid uncertainty during the approval process. The regulation also significantly increases and expands penalties for various violations. These penalties can be up to RMB 10 million ($1.44 million), or 5-10 times of any illegal gains that exceed RMB 1 million.

On the positive side, this regulation is designed to simplify the process for drug and medical device registration studies. It replaces an advance approval requirement with a notification process for any studies not involving the export of HGRs outside of China, although details of this notification process lack clarity at the present time.

5. Key Takeaways

The regulatory environment in China for MNCs is certainly getting tighter very quickly, especially with regards to data security, liability and international data transfer. For MNCs to be successful, they will need to keep track of legislative trends, especially recently published draft regulations by Chinese cybersecurity authorities.

This means that MNCs will need to adjust their global data protection strategies and prepare to move servers storing healthcare data into China. Contracts will need to be reviewed carefully between MNCs and network device/service vendors, data partners and clients – especially from a technical and managerial perspective. MNCs will also need to adjust their management strategy for internal system control, as well as conduct regular data protection audits and strengthen access control and personnel management. This will involve conducting regular training and preparing a response plan for potential data breach events.

Finally, MNCs will need to ensure that they obtain consent through contracts or other cooperation agreements. They'll need to clarify the rules, purposes, scope and other important aspects of data usage, and if the data usage activities are beyond the agreed scope, additional consent must be obtained. Importantly, MNCs must review cooperation agreements with research institutions in China to ensure they have the necessary qualifications to conduct research on certain types of data, such as HGRs. They also must conduct a security assessment review based on the requirements of government authorities, or obtain approval from government authorities, if required.

While these requirements may seem overwhelming at first glance, they are manageable if a company is prepared with a well-conceived plan for accessing the many benefits of the Chinese healthcare market.

© 2019 Kantar

References

- Cybersecurity law 2017 – [in English] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ [in Chinese] http://nic.hrbeu.edu.cn/_upload/article/files/4d/a2/543a91024b739b31ebe631355019/3d713f50-e1a0-45ec-83b1-46629106262d.pdf

- Real-world evidence supports basic considerations for drug development RWR Considerations (Guo Fa [2015] No. 44, May 2019) - http://www.cde.org.cn/news.do?method=viewInfoCommon&id=314865

- Healthcare Data Compliance in China - http://www.natlawreview.com

- China – Key Considerations in Using Real-World Evidence to Support Drug Development - https://www.chcuk.co.uk/?s=china

- Regulations on the Management of Human Genetic Resources (HGRs) (March 2019) - http://www.gov.cn/zhengce/content/2019-06/10/content_5398829.htm

KANTAR

Kantar is the world's leading data, insights and consulting company. We understand more about how people think, feel, shop, share, vote and view than anyone else. Combining our expertise in human understanding with advanced technologies, Kantar's 30,000 people help the world's leading organizations succeed and grow.

www.kantar.com/health