Published on *The National Law Review* https://natlawreview.com

Health Care Data Compliance in China: FAQ

Article By:

Carol B. Sun

Jenny Z.N. Chen

Data compliance in China's health care industry is multifaceted and highly sensitive, and applies to numerous types of data generated across the continuum of care. Multiple pieces of legislation prescribe complex regulatory requirements governing different types of data, and various supervisory authorities frequently conduct inspections and investigations, paying special attention to health care multinationals with operations in China.

This article provides a brief introduction to the regulatory requirements for health care data, along with key compliance steps for multinationals throughout the entire life cycle of health care data, including collection, storage, transfer and use.

IN DEPTH

1. What types of health care data are regulated in China? What are the key compliance points related to these types of health care data?

Data compliance rules apply to various sources and types of health care data, including medical record information, medical insurance information, health care logs, human genetic resources, medical experiments and scientific data. The table below lists the various types of health care data governed by China's laws and regulations related to health care and personal information, as well as the key regulatory compliance focus for each category.

Category	Definition	Key Regulatory Compliance Focus
Health Care Big Data The Administrative Measures on Standards, Security and Services of National Healthcare Big Data (for Trial Implementation)	Data relating to health care generated in the course of disease prevention and control as well as health management Note: the Measures do not clarify what data qualifies as health care "big" data.	Localisation and storage Transfer: Cross-border data transfer is subject to security assessment.

Human Genetic Resources The Interim Administrative Measures for the Management of Human Genetic Resources	Genetic materials and related information, including organs, tissues, cells, blood, preparations, recombinant deoxyribonucleic acid (DNA) constructs containing human genome, genes and their products.	Collection: Complex approval procedures are required, and collection by foreign entities or individuals is restricted. Localisation and storage Transfer: Approval from administrative bodies is required before cross-border transfer.
Pharmaceutical Data The Pharmaceutical Data Management Specification (Draft for Comments)	Data from all activities in a product's life cycle, such as R&D, production, circulation, post-marketing monitoring and evaluation.	Laws and regulations on personal information protection, health care big data protection and human genetic information protection, *etc.*, may apply under certain circumstances.
Medical Device Data The Guidelines for Technical Review of Network Security Registration for Medical Devices	Health care data and device data.	Laws and regulations on personal information protection, health care big data protection and human genetic information protection, *etc.*, may apply under certain circumstances.
Medical Records The Regulations for Medical Institutions on Medical Records Management	All texts, symbols, graphics, images and slides produced in medical activities by medical personnel, including outpatient (emergency) and hospitalisation medical records. Medical records are filed as medical history.	Collection: Consent from data subject is required. Transfer: Medical institutions should keep records strictly confidential except under specific circumstances.
Scientific Data The Measures for the Management of Scientific Data	Primarily data produced from basic research, application research, pilot development and other endeavours in such areas as natural science and engineering technology science, and the original data and data derived via observation and monitoring, survey and investigation, and inspection and detection that is used for scientific research activities.	Transfer: Data involving state secrets are strictly forbidden to be transferred to a third party.

2. What are the key compliance steps for health care data collection in China?

Collection of any health care data involving personal information should be based on the three principles of China's Cybersecurity Law (legitimacy, justification and necessity) and requires the consent of the data subject. The rules, purposes, methods and ranges of such collection should also

be disclosed to the data subject.

Collection of human genetic information by foreign entities or foreign individuals is strictly regulated, and such collection is subject to the approval of regulatory authorities.

Multinationals may wish to consider taking the following steps to be compliant with Chinese laws:

- For direct collection from data subjects, review the data collection agreements and clarify the purposes, rules, methods, ranges and other important aspects of collection disclosed to the data subject.
- For indirect collection (i.e., collection from business partners), review the partnership or delegation contracts to ascertain ownership of the health care data collected and ensure that the delegated party is compliant with Chinese cybersecurity laws and regulations.

3. What are the key compliance steps for health care data storage in China?

Multinationals should first focus on China's data localisation requirements. Chinese laws and regulations have strict requirements regarding storage of health care big data and human genetic information. Principally, health care big data and human genetic information must be stored in local, secured and trusted servers. Similar requirements are likely to expand to other types of health care data in the future.

Multinationals storing health care data in China should consider taking the following precautions:

- Keep an eye on legislative trends, especially recently published draft regulations by cybersecurity authorities.
- Adjust your global data protection strategy and prepare to move servers storing health care data into China.
- Review contracts between multinationals and network device/service vendors, especially from a technical and managerial perspective.
- Adjust your management strategy for internal system control.
- Conduct regular data protection audits and strengthen access control and personnel management.
- Conduct regular training and prepare a response plan for potential data breach events.

4. What are the key compliance steps for use and transfer of health care data?

The use, transfer or sharing of any health care data involving personal information with third parties requires the consent of the data subject. Alternatively, data may be de-identified to downgrade its sensitivity. For certain types of health care data, such as health care big data and human genetic information, security assessments review or approval from administrative authorities will apply prior to cross-border transfer.

Multinationals should considering taking the following steps before transfer:

- Ensure consent is obtained through contracts or other cooperation agreements.
- Clarify the rules, purposes, scope and other important aspects of usage. If the data usage activities are beyond the agreed scope, additional consent must be obtained.
- 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 human genetic resources.
- Conduct a security assessment review based on the requirements of government authorities, or obtain approval from government authorities if required.

National Law Review, Volume IX, Number 162