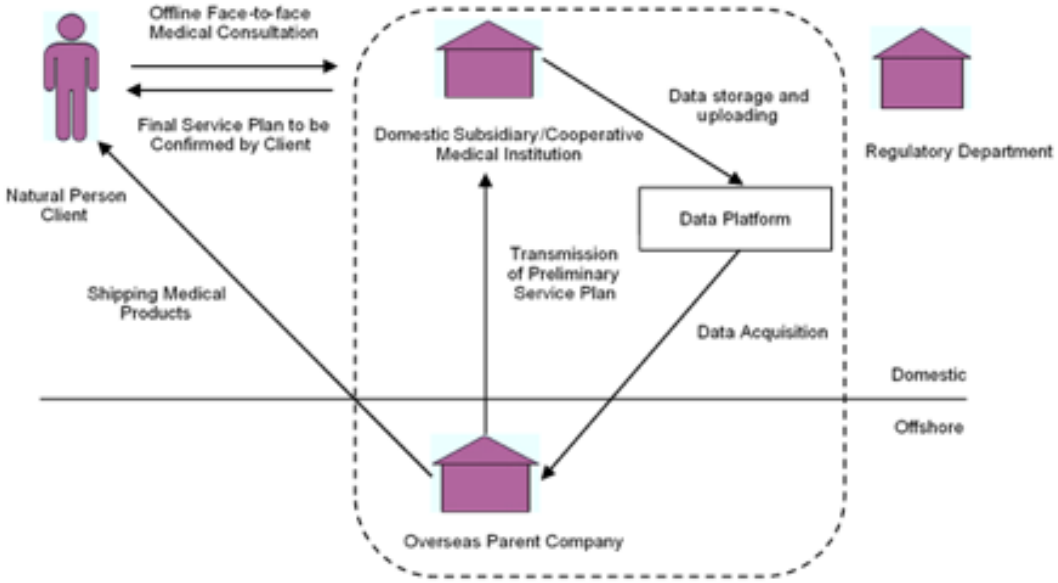
大成 DENTONS

Practice/Industry sector: Competition and Antitrust/Privacy and Cybersecurity

Grow | Protect | Operate | Finance

Sort date: 2021.12.03

In the first two articles of this series, we discussed how internet medical enterprises collect, store and share healthcare data within China in compliance with laws and regulations based on the circumstance where a multinational medical product manufacturer achieved data interconnection and information sharing through its internal data platform. This article will discuss the third step of the data flow chart under this circumstance, that is, the domestic internet medical enterprise transmits personal healthcare data to its overseas parent company.



1. Whether or not a domestic subsidiary of a multinational company ("MNC") can transmit personal healthcare data to overseas recipients?

The currently effective laws and regulations such as the Personal Information Protection Law, the Data Security Law and the Cyber Security Law do not completely prohibit the domestic subsidiaries of MNCs from transmitting personal healthcare data to overseas recipients. In compliance with PRC laws and regulations as well as regulatory requirements, domestic subsidiaries of MNCs may provide their overseas parent companies with healthcare data they have collected in China.

However, with respect to certain types of personal healthcare data, the transmission from domestic subsidiaries of MNCs to overseas recipients is prohibited by PRC law. Such prohibition applies to the personal healthcare data involving national secrets and information of human genetic resources.

In addition, the Data Security Law also provides for a data hierarchical and classification protection system, and requires all competent governmental authorities to prepare a specific catalogue for important data of each governmental authority as well as relevant industries and fields and give priority to the protection of important data listed in the catalogue. However, so far, the relevant governmental authorities have not yet formulated a catalogue for important data in the healthcare field, and it is possible that more types of healthcare data will be protected as important data and even prohibited from cross-border transmission after such specific catalogue is formulated.

2. What rules shall be followed before cross-border transmission of personal healthcare data?

Personal healthcare data is sensitive personal information. According to the relevant provisions of the Personal Information Protection Law, before outbound transmission of such data, the domestic subsidiary of an MNC, as a data processor, shall inform its natural-person clients and obtain their consents, conduct impact assessment on personal information protection beforehand, do security assessment on information outbound transmission, obtain certification of personal information protection, and enter into contracts related to data outbound transmission with the overseas recipient.

a. Informing involved individuals and obtaining their consents

   Cross-border transmission of healthcare data falls within the scope of cross-border transmission of personal information. According to the Personal Information Protection Law, the domestic subsidiary of an MNC shall, before transmitting personal information to overseas recipients, inform the involved individual of the name and contact information of the overseas recipients, the purpose and method of processing, the type of personal information, and the method and procedure for the involved individual to exercise his right to know and make decision, and his other rights as stipulated in the Personal Information Protection Law against the overseas recipients, and obtain the involved individual's separate consent.

b. Conducting an impact assessment on the personal information protection beforehand and recording the handling results

   According to the provisions of the Personal Information Protection Law, a domestic subsidiary of an MNC shall, prior to providing personal healthcare data to overseas recipients, conduct a prior impact assessment on the personal information protection. The generated report on the impact assessment of personal information protection and the records of handling shall be kept for at least three years.

   It is noteworthy that the impact assessment report of personal information protection may affect the scope, method and scale of cross-border transmission of personal healthcare data. According to the Administrative Regulations on Network Data Security (Draft for Comments), the domestic subsidiary of an MNC is not allowed to transmit healthcare data beyond the purpose, scope, method, data type and scale specified in such impact assessment report submitted to cyberspace regulating authorities.

c. Security Assessment for Outbound Transmission

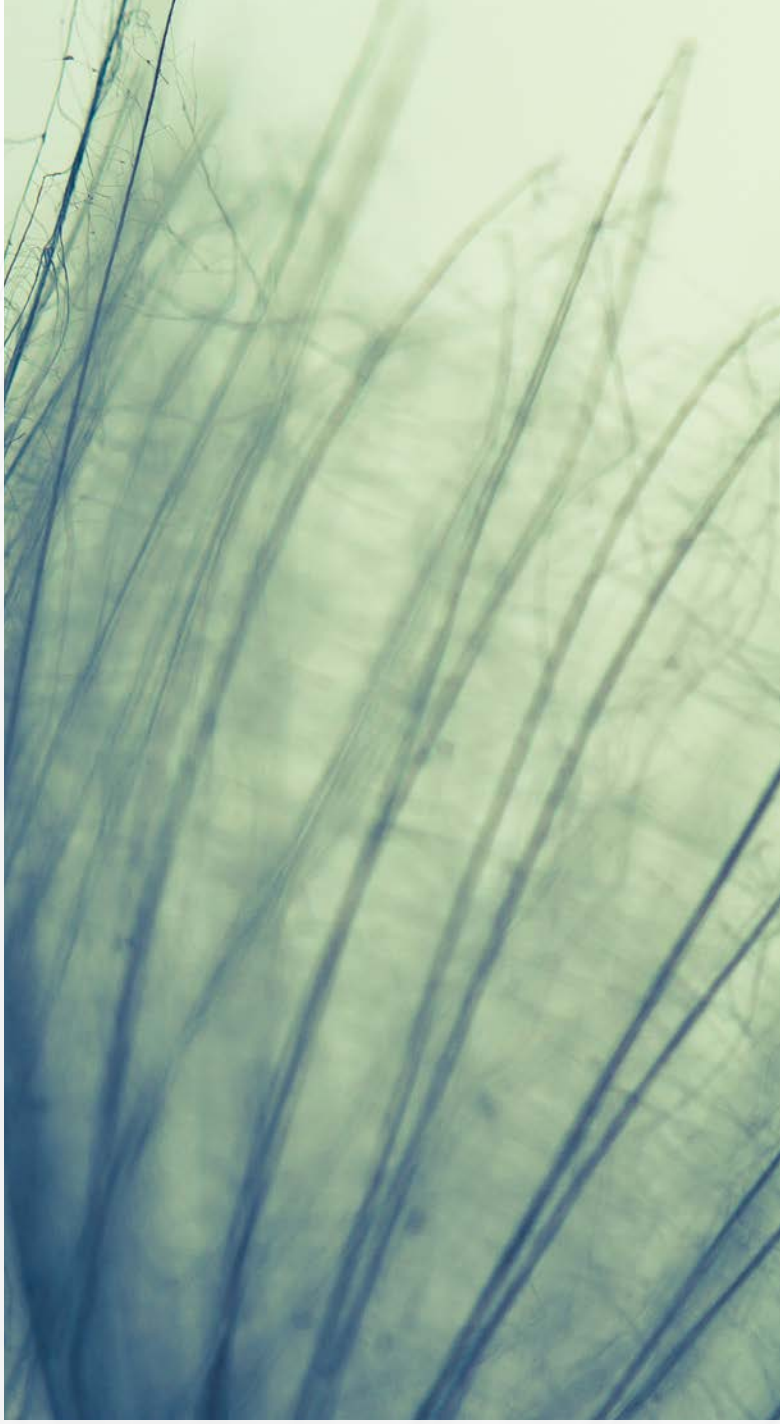
The Measures for the Security Assessment of Outbound Transmission of Data (Draft for Comments), drafted by the Cyberspace Administration of China (hereinafter referred to as "CAC"), attempts to clarify the specific requirements for data export security assessment. Before transmitting personal health and medical data abroad, a domestic subsidiary of an MNC shall carry out the self-assessment of the risks of outbound data transmission, and then apply to CAC for security assessment of outbound data transmission through the local cyberspace regulating authorities at the provincial level. The scope, method and scale of the personal health and medical data to be transmitted abroad shall not exceed the purpose, scope, method, data type and scale specified in the assessment report.

d. Personal information protection authentication

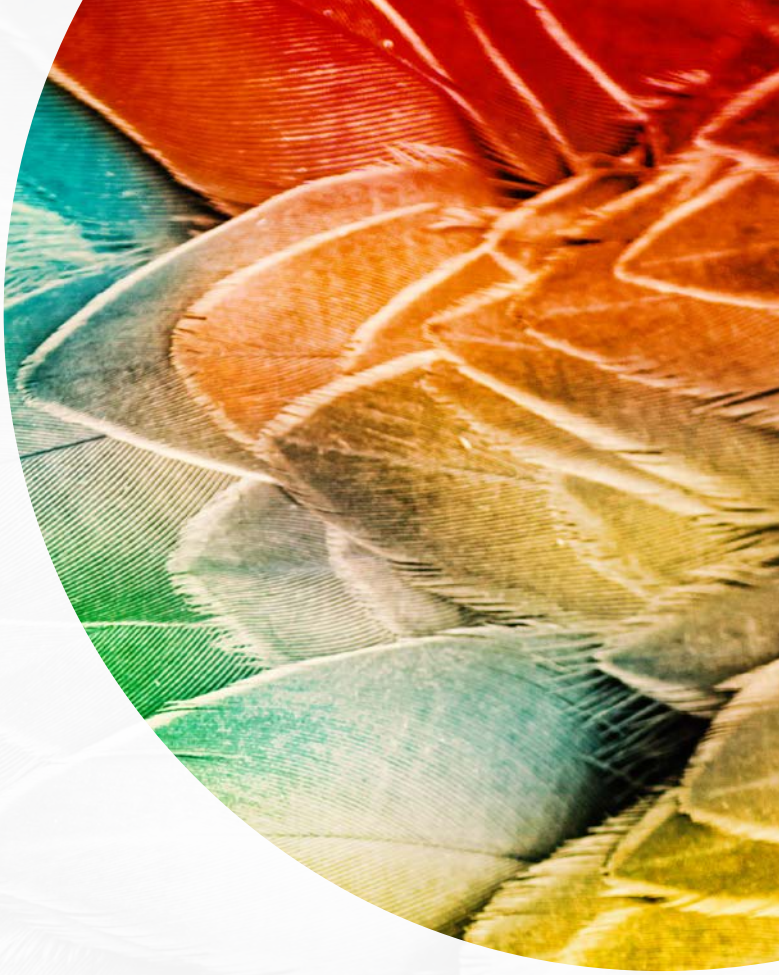
According to the Personal Information Protection Law, domestic subsidiaries of MNCs shall obtain personal information protection authentication from professional institutions in accordance with the regulations of the CAC before transmitting healthcare data abroad. A domestic subsidiary of a MNC that has passed the authentication of the personal information security management system issued by the China Cybersecurity Review Technology and Certification Center may meet the requirements of personal information protection for cross-border transmission of healthcare data.

e. Signing a data export contract

The Personal Information Protection Law, the Measures for the Security Assessment of Outbound Transmission of Data (Draft for Comments) and the Administrative Regulations on Network Data Security (Draft for Comments) all require that a personal information processor shall sign a data export contract with the overseas data receiver, take effective measures to supervise the data receiver to use the data according to the purpose, scope and method as agreed by the two parties, and perform the obligation of data security protection to ensure data security.



Currently, the relevant authorities have not issued a sample data export contract. However, the CAC emphasizes in the Measures for the Security Assessment of Outbound Transmission of Data (Draft for Comments) that a data export contract shall fully specify the responsibility and obligation of data security protection, and CAC gives suggestions on the terms and conditions of the contract. With regard to the cross-border transmission of healthcare data, it is possible that the competent health authorities may formulate a special data export contract based on the characteristics of the healthcare industry and the personal healthcare data. We will wait and see.



3. What obligations shall domestic subsidiaries of MNCs perform after the personal healthcare data is transmitted abroad?

The Administrative Regulations on Network Data Security (Draft for Comments) , recently issued by the CAC, sets out the obligations of domestic entities after the data is transmitted abroad, including:

a. Accepting complaints and compensating losses

After the personal healthcare data is transmitted abroad, the domestic subsidiaries of MNCs shall accept and handle the complaints of users; if the data is transmitted abroad and causes damage to the legitimate rights and interests of individuals and organizations or public interests, the domestic subsidiaries of MNCs shall be liable according to the applicable law.

b. Obligation of archiving

After the personal healthcare data is transmitted abroad, the domestic subsidiaries of MNCs shall keep the relevant log records and approval records for transmitting the data abroad for at least three years.

c. Obligation of cooperation in investigation

When the CAC, in concert with the relevant departments of the State Council, examines the type and scope of the personal information and important healthcare data transmitted abroad, the domestic subsidiaries of MNCs shall display the information in a plain-text and readable way. If the CAC deems that the data is not allowed to be transmitted abroad, the domestic subsidiaries shall stop transmitting, and take effective measures to remedy the security of the personal healthcare data that has been transmitted abroad.

d. Obligation for re-transmission of data

If it is indeed necessary to re-transmit the personal healthcare data abroad, the domestic subsidiaries of MNCs shall reach an agreement with the natural person clients in advance on the conditions for re-transmission and specify the security protection obligations of the receiver of the personal healthcare data.

e. Obligation of reporting

Personal healthcare data is personal information. The domestic subsidiaries of MNCs that transmit the personal healthcare data abroad shall prepare a data export security report before January 31 each year and report the information about the data export in the previous year to the cyberspace regulating authorities at the level of city divided into districts.

To sum up

To sum up, in the process of cross-border transmission of personal healthcare data to its overseas parent company, the domestic subsidiaries of MNCs shall comply with and perform the obligations of maintaining the security of clients' data and privacy, and maintain the compliance and legitimacy of data processing at all times while achieving their business objectives and pursuing business value. This article is the third one in a series on healthcare data compliance, and we will further analyze and discuss the data compliance issues involved in the subsequent steps under the data transfer chart on the home page. Please stay tuned!

CSBrand-86138-Healthcare Data Compliance Series ( ) — 19/04/2022