How Should Pharmaceutical Companies Deal with China's New Data Export Regulations?

Kevin Duan and Kemeng Cai, of Han Kun Law Offices, discuss Chinese data protection regulation and its effect on the pharmaceutical industry in China.

Published on 17 October 2022.

***Kevin Duan**, Partner*

Han Kun Law Offices

***Kemeng Cai**, Partner*

Han Kun Law Offices

This article is published by Chambers as an expert focus:
https://chambers.com/legal-trends/chinas-data-export-regulations

On July 7, 2022, the Cyberspace Administration of China (the "**CAC**") formally issued the long-awaited *Measures for Security Assessment of Cross-border Data Transfers* (the "**Assessment Measures**"). The Assessment Measures specify circumstances where exports of data are subject to CAC's security assessment ("**Security Assessment**"), including:

- data handlers who export important data;
- critical information infrastructure operators or personal information handlers who export personal information and have processed the personal information of at least 1 million individuals;
- data handlers who have cumulatively exported personal information of at least 100,000 individuals or sensitive personal information of at least 10,000 individuals since January 1 of the previous year;
- other circumstances where an application for Security Assessment is required as prescribed by the CAC.

The Assessment Measures have come into effect on September 1, 2022, and they grant a grace period of six months therefrom for a data handler to rectify data exports not in compliance with the requirements of the Assessment Measures.

What Does the Security Assessment Look Like?

Data handlers must carry out a self-assessment before applying for the Security Assessment, which will be the core of the Security Assessment. The matters to be covered in the self-assessment mainly include:

- the legality, legitimacy and necessity of the export as well as the purpose, scope, and method of the data processing of overseas receivers;
- the quantity, scope, type, sensitivity and risk of data exported;
- the protection capabilities of overseas receivers;
- security risks during and after data cross-border transfer and the protection of personal information rights and interests; and,
- contractual arrangements governing the responsibilities and obligations of both parties for data security and protection in contracts or other legally binding documents drawn up for the data export.

The CAC Security Assessment will be largely based on paper review of the self-assessment, and some additional factors to be evaluated in the Security Assessment include whether the laws and regulations of the receiving country provide adequate level of protection equivalent to that under the PRC laws.

Security Assessment Procedure and Timelines?

The application of security assessment should be submitted to the provincial CAC for procedural review, and if the provincial CAC confirms the application materials are complete, it will forward the materials to central CAC for further formal review. Once central CAC accepts the application, it should complete the assessment within 45 business days, which can be extended in case of complexity. The entire application is expected to take around 2-3 months.

How the Assessment Measures Interplay with Other Recent Data Export Regulations

The Assessment Measures are the high tide among a series of regulations on cross-border data transfer issued in recent days, which mainly include:

- On April 29, 2022, the National Information Security Standardization Technical Committee issued for public comments a draft of the *Technical Specifications for the Certification of*

Personal Information Cross-border Processing (the "**Draft Specifications**"), which outlines the framework for the voluntary certification for cross-border processing of personal information among multinational group companies.

- On June 30, 2022, the CAC issued the *Provisions on the Standard Contract for the Export of Personal Information* (*Draft for Comment*) and the *Draft Standard Contract for the Export of Personal Information* (the "**Standard Contract**") which clarifies the application scope, conditions of application and the main contents of the China version standard contract for personal information export.

For other data export circumstances not triggering the Security Assessment, data handlers may transfer personal information outside of China upon entering into the Standard Contract with the overseas receivers or upon completing the security certification by government designated certification agencies if the transfer is among affiliates within multinational group companies.

Besides, according to *the 2019 Regulations on the Management of Human Genetic Resources* and *the draft Detailed Rules for the Implementation of the Regulations on the Management of Human Genetic Resources* (the "**Rules**") issued by the Ministry of Science and Technology ("**MOST**") for public comment, provision of human genetic resources ("**HGR**") information to foreign entities or individuals or entities under actual control by such foreign entities/individuals shall be filed with MOST for record. As exceptions, where such outbound provision may endanger China's national security, public health and public interest, for example, HGR information of important genetic families, HGR information in specific regions, or exome sequencing and genome sequencing information resources for people with more than 500 people, the provision must pass the national security assessment by MOST. Since HGR information may also constitute personal information or even important data, the restrictions on export of HGR information under the HGR regulations may overlap with the data export regulations such as the Assessment Measures. Currently, pharmaceutical companies should apply to both MOST and CAC if the export of HGR meets the triggering conditions under the HGR regulations and data export regulations.

When Pharmaceutical Companies May Need to Submit Security Assessment Application

Cross-border data transfer is crucial for multinational pharmaceutical companies' business and operation in China. Pharmaceutical companies may need to apply for Security Assessment if their data export meet the threshold under the Assessment Measures, and common data export scenarios mainly include-

- Multi-Centre IND and NDA Application Data: Multinational pharmaceutical companies usually need to submit a variety of information when submitting investigational new drug

(IND) and new drug applications (NDA) with respective administrators in different jurisdictions, which may contain preclinical data, manufacturing information, clinical protocols, investigator information, pharmacology and toxicology data, non-clinical pharmacological and toxicological information, human pharmacokinetic (PK) and bioavailability information, microbiology, clinical information, safety update, statistical information, patent and exclusivity information, etc.

- Data Processed by Foreign EDC System Suppliers: Use of Electronic Data Capture (EDC) systems to process clinical trial data by pharmaceutical companies has become increasingly prevalent in recent years. For foreign EDC suppliers, their EDC systems may be hosted abroad thus may cause their clients' clinical trial data to be exported outside of China. Please kindly note that coded clinical data without any direct identifier may be deemed as de-identified information rather than anonymized information, thus still constitutes personal information under PRC laws and is subject to the data export regulations.

- International Collaborative Research Data: Foreign organisations and individuals are permitted to use HGR collected in China for scientific research purposes in co-operation with a Chinese scientific research institution, college, university, medical institution or enterprise. Such international collaborative research usually entail the export of HGR information.

- Internal Management Data: Like most multinational companies in other industries, multinational pharmaceutical companies also rely on global deployed HR, financial, client relation, office and other backend systems to support their daily operation, which may entail cross border transfer of personal information of employees, suppliers, healthcare professionals and etc.

How Pharmaceutical Companies Should Prepare for the Security Assessment?

Security Assessment requirements propose unprecedentedly strict restrictions on the export of data from China mainland. To address the compliance challenges posed by the recent data export regulations, it is advisable for pharmaceutical companies to consider the following suggestions:

- pharmaceutical companies are advised to carry out data mapping, complete rectifications when necessary, and apply for a Security Assessment for required data export scenarios as early as possible. Theoretically, companies need to obtain approvals for data export, if applicable, before Mar 1, 2023, when the cure period expires. Data exports subject to Security Assessment yet without an approval before the expiration of the cure period will be deemed illegal and may lead to severe consequences under relevant PRC data laws.

- pharmaceutical companies who intend to carry out data export activities in the future are advised to formulate an internal data export identification system and a self-assessment system, and to prepare relevant data export contract, privacy policies, informed consent forms and other legal documents in advance, which will serve as key components to smoothly promote data export activities.

- the Assessment Measures set low quantity thresholds for the mandatory Security Assessment. As a result, pharmaceutical companies may consider localization as an option to avoid lengthy assessment procedures and the uncertainty that they bring, especially for export of large volume of sensitive personal information such as healthcare data and HGR information.