DS NEWSLETTER savoir, faire
NEWSLETTER – LEGAL INFORMATIONS
PROPOSED BY DS AVOCATS

Health data : control your risks !

ASIE

BACKGROUND

In recent years, with China's government vigorously implementing a series of policies such as *"Internet+ Healthcare"*, hospitals, medical institutions and even medical equipment suppliers have gradually digitalized. However, while medical digitization brings convenience, it also raises the risk of data leakage of personal information which are particularly sensitive for individuals.

Indeed, health data may be the most comprehensive record with personal data of a data subject. It may include sensitive personal data, such as information related to the past, current, and future physical or mental health status of an individual, but also other information provided to the medical institutions during the patient's medical journey, such as bank account information, credit card number, etc. Once leaked, it may not only bring negative impact on the privacy of the relevant data subjects, but it can also incur property losses.

INTRODUCTION OF THE HEALTH DATA STANDARD

Fortunately, in 2021, China issued a series of laws, regulations and national standards on personal data.

In addition to the well-known Data Security Law ("*DSL*") and Personal Information Protection Law ("*PIPL*"), a national standard with practical guiding role, "*Information Security Technology-Guide for Health Data Security*" (GB / T 39725-2020) (the "*Standard*") came into effect on July 1, 2021.

PIPL enshrines the sensitive data status of health data, and sets some requirements for the processing of such sensitive data, but does not elaborate much further. The national standard goes deeper into the specific requirements taking into account different scenarios and data type.

- First, the Standard defines "*health data*" as "*personal healthcare data and the healthcare-related data processed from personal healthcare data, including overall analysis results for groups, trend predictions, disease prevention and treatment statistics, etc.*".

- Besides, it summarizes the recommended security measures for personal data in common healthcare scenarios, including hospital cooperation, telemedicine, data collection, health sensing data management, mobile applications, clinical research, commercial insurance, remote maintenance of medical devices, etc. As for recommended technical measures, it includes internal organization management, data classification, access control, user right management, encryption control, equipment protection, network security management, data external cooperation management, de-identification guidance, etc.

- In addition, it suggests management of health data by classification, which is consistent with the requirements of the *PIPL*, *Data Security Law* ("*DSL*") and *Cyber Security Law* ("*CSL*") regarding (personal) data management.

In order to differentiate and refine the security requirements for different usage scenario of the data, the Standard divides health data into six categories :

1. personal identity data (such as name, ID card, telephone, etc.);
2. health status data (such as medical history, test data, etc.);
3. medical application data (such as outpatient medical records, admission records, etc.);
4. medical payment data (such as medical insurance payment information, transaction amount, insurance status, etc.);
5. health resource data (hospital basic data, hospital operation data, etc.); and,
6. public health data (such as infectious disease epidemic data, birth and death data).

- According to the importance and the level of risk, this Standard also divides health data into five levels. From level 1 to level 5, the requirements of restrictions and control measures becoming stricter gradually.

- In addition to being consistent with the upper law in terms of hierarchical and classified management system, this Standard further refines the relevant rights and requirements of data subjects, for example, it stipulates that data subjects have access and query rights, access to copies, correction and supplement rights, and backtracking query rights (that is, the data subject has the right to conduct historical backtracking query on the use or disclosure of data by the controller or its processor, with a minimum backtracking period of six years).

- It is worth noting that this Standard introduces a new concept of "*data user* ", which does not appear in the *PIPL*. The data user is not the data controller or data processor, nor the data subject. The data user is mentioned in some scenarios of use of certain health data (e.g. for hospitals who need to conduct internal audit, the auditor would be considered as data user). The obligations of the data user vary depending on the scenario, and the type and level of the data they are using.

- In addition, due to the particularity of the medical scene, this Standard also defines four situations in which the data controller can use or disclose personal health data without the specific consent of the data subject :

1. when it is provided to the data subject her/himself;
2. for treatment, payment or health care;
3. when public interest is involved or when required by laws and regulations;
4. when limited Data Sets are used for scientific research, medical / health education, public health purposes. (Limited Data Set refers to the personal health data set that has been partially tokenized, but recognizes and identifies the corresponding individual and therefore needs to be protected. In the above cases, the data controller can rely on legal and regulatory requirements, professional ethics, ethics and professional judgment to determine which personal health data are allowed to be used or disclosed.)

- Data export: the Standard makes it clear that the data controller shall not store health data in an overseas server. Export of personal health data outside of China is possible (for example for academic research purposes) but upon certain requirements (de-identification, approval of the security committee or the relevant government departments depending on the importance and volume of the data). In all cases, specific consent of the data subject is also necessary.

SUGGESTION

Since the *PIPL* is not clear enough in terms of some compliance requirements, at least for health data, this Standard has " translated " general legal obligations into detailed guidelines, which is practical enough for health data controllers, processors, and data users to follow. We recommend that health care professionals, medical institutions and other medical related entities carry out compliance work according to the requirements of the standard as soon as possible.

For any additional information please contact:

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
DOYON@dsavocats.com