The Impact of the Personal Information Protection Law on Life Science Business

By Xun Yang | Sherry Xia

The Personal Information Protection Law ("PIPL") came into effect on 1 November, 2021. It is the first comprehensive legislation on personal information protections. It will have significant impact on business, including, in particular, life science business.

1. An introduction to PIPL and to Personal Information Protection Regime

PIPL was first included in China's legislative agenda in September 2018. After three rounds of deliberations and public consultations, PIPL was approved on the 30th meeting of the Standing Committee of the 13th National People's Congress in August 2021, and officially came into effect on 1 November, 2021.

PIPL, as a fundamental law in the field of personal information protections, consolidates piecemeal legislations on personal information protections and unifies the personal information protection rules regardless of whether personal information in electronic forms or on papers, about consumers or employees, is concerned. It strengthens the personal information protection requirements and also imposes heavier penalties on violators.

PIPL is a milestone legislation on personal information protections but it is not the only legislation. Some other laws and regulations also have provisions on personal information protections. For example, the Civil Code recognizes interest in personal information as a type of personal right; the Criminal Law criminalizes illegal acquisition and sales of

如果您需要本出版物的中文本，
请联系:

Publication@llinkslaw. com

For more Llinks publications,
please contact:

Publication@llinkslaw.com

personal information. The Telecoms User and Internet User Personal Information Protection Rule issued by the Ministry of Industry and Information Technology (MIIT) in 2013 applies to the collections and processes of personal information via Apps and other internet portals. Besides, in the life science sector, relevant regulators issue rules to protect personal information within their respective authority. For example, the National Healthcare Commission (NHC) issued the Administrative Measure for Population and Healthcare Information in 2014, which has provisions on protecting patient data; and the National Medical Product Administration (NMPA) amended its Drug Clinical Trial Quality Management Specification in 2020 to include the protection on personal information of the subjects. As such, life science companies would need to consider all these laws, regulations, and rules when determining their personal information protection practice.

2. A Prospective View of Enforcing PIPL

As various laws and regulations have provisions on protecting personal information, various government agencies will participate in enforcing personal information protection laws. According to PIPL, the Cyberspace Administration of China ("CAC") will be responsible for coordinating the protection of personal information and related supervision and management. MIIT will enforce the data protection rules on collections and processes of personal information via Apps and internet portals. Relevant departments of the State Council are responsible for protecting, supervising the protection of personal information within their respective vires. For example, NHC will enforce the personal information protection rules in the medical service context and NMPA will exercise their power to protect personal information in clinical trial, drug registration, and AE reporting context.

Under PIPL, the legal consequence for violation personal information protection requirements became more serious than before. PIPL impose increased penalties for infringement of personal information, including an administrative fine of up to RMB 50 million or 5% of the violator's turnover in the preceding year, confiscation of illegal gains, cessation of operation for rectification, or revocation of operating permits or business licenses. Additionally, the person-in-charge or other directly liable individuals may also be held liable and subject to a fine up to RMB 1 million. Such individuals may further be restricted from serving as a director, supervisor, senior management or personal information protection officer for a certain period of time, and if a crime is constituted, criminal liability shall be investigated in accordance with the law.

Infringement of personal information, causing damages to relevant individuals, will result in civil liabilities. What's important, PIPL shifts the burden of proof of "fault" on the personal information handlers to facilitate the establishment of a personal information infringement claims. According to the PIPL, in case of personal information infringement, if the party which handles personal information fails to prove its innocence, it will be presumed to be faulty.

Additionally, PIPL also stipulates that any illegal act of personal information by personal information processors will be recorded in credit files and disclosed to the public. This will cause serious negative impacts on their reputation, damage their public image and thus influence their business operation.

PIPL has particular impact on the life science sector. The life science sector is one of the industries where sensitive personal information is intensively processed, pharmaceutical companies, medical device companies and healthcare service providers not only collect and store a huge number of patients' and medical professionals' personal information, but also often handle sensitive healthcare related information and even human genetic resources and population health information which are crucial to the public interest and national security. It is expected that the government will focus the enforcement of PIPL on, among others, the life science sector.

Moreover, with the booming development of online business during recent years, telecoms technology is increasingly used in the life science sector, thus boosts the digital healthcare business, including online hospital services, online prescription, remote medical device, digital therapy. Apps, remote devices, and other terminals are widely used to collect, store, process, and transfer a large amount of personal information. PIPL would need to be observed to ensure the compliance to protect patients and HCP's personal information.

3. Challenges to Life Science Business

PIPL imposes strict requirements on operators of life science business in terms of collection, process, storage, and transfer of personal information.

1) Personal Information Collection

Scenarios for information collection on healthcare and life science areas include: diagnosis and treatments, health consultation for individuals, clinical trials of drug research and development ("R&D"), medical accident reporting, adverse effect reporting; health insurance and life insurance claims, etc. In these scenarios, online and offline life science business operators and institutions will necessarily handle personal information and even sensitive personal information, such as health status information, medical application information, medical payment data, etc.

According to PIPL, the collection of personal information must have a clear and reasonable purpose and be limited to the minimum scope for achieving the purpose. Excessive collection of personal information is not allowed. Besides, where the handling of personal information is based on the individual's consents, such consents must be voluntary and explicit on the premise that the individual is fully informed of the purpose, method and range of use. In addition, the handling of sensitive personal information (which include health related information) requires sufficient necessity and separate consents. Moreover, to collect personal information of a minor under the age of 14, personal information handlers must obtain the consents of the minors' parents or other guardians.

These requirements, although looks straight forward, may present challenges to life science business. Firstly, pharmaceutical companies, which have needs to collect patient information, may

not have direct access to patients due to compliance requirements, which creates difficulties for pharmaceutical companies to seek consents from patients. Secondly, in the case where pharmaceutical companies which seek collect information directly from patients (e.g., via Apps or other internet portals), patients information is sometimes provided by their relatives; this create challenges as to how companies can ascertain that these relatives have the due authorization to provide such information. Thirdly, with respect to scientific studies, research institutions (including R&D divisions of pharmaceutical companies) may collect a wide range of information from those subjects without a clear objective (but with a rough orientation). Thus, arises the question whether the collection of information without specific experimental objective satisfies "clear purpose" requirement for consents.

2) Possession of Personal Information

According to PIPL, a personal information handler must (1) adopt proper measures (including managerial measures and technical measures) to protect the personal information in its possession; (2) must not retain personal information which it collects for a period exceeding the minimum period necessary for achieving the purpose notified to individuals; (3) must classify the personal information in its possession and apply proper protective measures.

These obligations require life science companies to take actions to protect the personal information they collect and generate during their course of business. Firstly, when a pharmaceutical company receives information about patients, the information may be used for AE reporting, for patient care services, for internal management, etc. Different divisions would need different section of information to achieve their respective function. This requires the companies to establish an internal control system, granting different divisions only authority to access to information on a need-to-know basis. Secondly, some health related data collected during researches or otherwise about use of drugs which have already been authorized for sales may be stored for a long period of time without a specific objective with the expectation that they may be useful in future studies. Question is whether this practice violates the minimum period requirement. Thirdly, some healthcare related data are subject to regulatory restrictions. For example, medical records are required to be stored in HIS, resulting in difficulties to connect healthcare service provider to share medical records with hospitals.

3) Transfer of personal information

Under PIPL, there are four types of personal information transfers, being: (1) joint handling of personal information, (2) provision of personal information, (3) entrusted handling of personal information, and (4) personal information transfers in a business transfer context. PIPL imposes different requirements, such as notification, separate consents, etc. on personal information transfers in different scenarios in order to ensure the security levels of personal information protections will not be prejudiced because of the transfers.

Life science companies may encounter personal information transfers in various scenarios. However, it is often unclear which category the transfer would fall within. For example, pharmaceutical companies usually distribute drugs through distributors and engage distributors to collect certain patient data (especially when the distributors deliver drugs to patients). In this scenario, the relationship between the pharmaceutical companies and the distributors could be a "provision of personal information" or an "entrusted handling of personal information" depending on which party determines the scope of the collection and be responsible for the patients' information collected. For another example, when a pharmaceutical company engages hospitals to perform clinical trials, the relationship vis-à-vis information about the subjects may not be necessarily an "entrusting" relationship because the hospitals have their own standing to collect personal information about the subjects.

4) Export of personal information

Most multinational companies would face the data exportation issue because they process personal information collected or generated in China on a global basis. Under PIPL, export of personal information must meet one of the following conditions: (1) passing security assessment by CAC; (2) being certified by qualified institutions; or (3) entering into a data transfer agreement with the recipient of personal information in a standard form stipulated by CAC. Additional, a personal information protection impact assessment is required before the relevant personal information being exported. However, despite of the effectiveness of PIPL on 1 November 2021, no security assessment procedure or certification procedure has been established; nor has CAC released the standard personal information export contract. How can companies continue exporting personal information at possibly lowest level of risk?

There are a number of scenarios where life science companies would need to export personal information outside of China: (1) for globally authorized drug, adverse effects may need to be reported to authorities in multiple authorities and thus incur personal information export; (2) for multi-site clinical trials or pre-clinical trials, information about subjects may need to be processed globally, thus incur personal information export; and (3) with respect to multi-national life science companies, employee data may also need to be exported for centralized management. A process needs to be established to notify the relevant individuals of the export and to seek their consents. Additionally, an internal risk assessment procedure is advisable in order to mitigate compliance risks.

4. Suggested Approach to Comply with PIPL

PIPL has come into effect on November 1. There is no grace period for the enforcement. Whilst it may take time for life science companies to fully digest the requirements under PIPL and implement them, the government will not too long to enforce PIPL. How can life science companies act to mitigate the risks from failure to comply with PIPL?

1) Establishment of data governance

Internal data governance is advisable to be established to effectively manage the handling of personal information. The governance needs to cover: (1) policies relating to management of personal information, covering contents stipulated by laws; (2) a department or a person in charge of personal information protections; and (3) trainings to improve employees' personal information protection awareness. These governances, for one thing, help mitigate data breach risks; and for another, form a defense that the companies have acted diligently to protect personal information. Thus, in case a company is sued for a personal data incident, well-established governance (and the record of performance of the governance) will form an evidence of "no fault."

2) Internal Audit

Life science companies may consider performing internal audits, which audits may serve two purposes, being (i) identification of potential loopholes with PIPL requirements and (ii) record well observation of PIPL and internal protection policies enacted under PIPL. As discussed above, PIPL may challenge personal information practice in various aspects, an internal audits will identify the non-compliance so as for life science companies to remedy it. If an internal audit proves that a life science company complies with PIPL from all aspects, the report of the internal audit will form an evidence to demonstrate that the company has no fault in a potential investigation or a potential civil litigation on personal information protection matters against it.

3) Re -stream of business process

When an audit reveals non-compliance, life science companies would need to take remedial measures. PIPL imposes strict requirements on handling of personal information and, thus, may incur necessity to change the current data practice by life science companies. For example, given the difficulties to seek patients' consents to collect their information directly in hospitals, life science companies may consider launching a patient care platform to attract patients to register on it and to seek patients' consents on that platform. For another example, with respect to remote healthcare business, companies may consider moving their regional hubs into China to store healthcare related data to mitigate data export implications.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI

19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road, Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD