LLINKS Law Offices
通力律师事务所

**SHANGHAI**
16F/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

**HONG KONG**
27F, Henley Building
5 Queen's Road Central
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

**Llinks Law Bulletins | Life Science**

**April 2020**

# Compliance Tips for Medical Health APPs (Part II) - Personal Information Collection and Use

**By David Pan | Susan Deng**

## Series Foreword

The Internet has been changing our lives at an unprecedented pace. In addition to E-shopping and food delivery, Internet medical services have become a significant part of our life. People start trying online diagnosis services when they feel sick; when they visit a doctor, they make online appointments beforehand; people also buy pharmaceuticals online as opposed to from brick and mortar pharmacies. Moreover, Internet medical services have permeated into our life, largely unnoticed. Our watches can measure our heart rate, electrocardiograph and even blood pressure, and more and more medical tests and assessments that were only available at hospitals can now be done remotely from home.

In tandem with growth opportunities, the fast-developing Internet medical technologies also pose new compliance challenges to business operators. What is the scope of legitimate online drug sales? Can prescription drugs be sold online? What telecommunication permits and approvals are required for online diagnosis, registration and sales via an APP? Do APPs and devices that feature medical monitoring or testing constitute medical devices? What are the requirements on drug transportation and logistics? How to protect personal information in Internet medical services? These are all common questions related to Internet medical services, yet their answers are far from clear to those who run the businesses.

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

Based on our law practices, we have prepared a series of articles in relation to Internet medical services, in the hope to help healthcare businesses to better understand relevant legal framework and regulatory trends. **This article is the third of the series: Compliance Tips for Medical Health APPs (Part II) - Personal Information Collection and Use.**

With the rapid development of big data, cloud computing, Internet of Things, artificial intelligence and other technologies, the Internet medical market has been booming, and "Internet + Medical Health" has become an investment hotspot among public medical institutions and pharmaceutical companies. The data from Qianzhan Industry Research Institute shows that the scale of China's Internet medical market is expected to reach RMB 90 billion in 2020. As an important branch of Internet medical industry, mobile health plays a significant role in improving patient experience, reallocating medical resources, and enhancing health management.

Mobile health refers to the healthcare services supported by mobile internet technology and provided by various mobile internet platforms. Among various forms of mobile health services, medical health Apps are most typical. The functions of such Apps have basically covered the entire medical treatment process from pre-diagnosis to post-diagnosis, including online inquiry, pre-diagnosis consultation, online registration, online payment, online query of test results, health education and management, doctor-patient communication, post-diagnosis follow-up, data collection, chronic disease management, remote monitoring, Internet drug sales, doctors or patients communities. As the functions, requirements, and business models of medical health Apps are becoming increasingly diverse, the channels and types of data collected by Apps, and the purpose and methods of collecting and processing have become more complicated. Combining laws and regulations with our law practice experience, the authors will analyze the compliance tips for medical health Apps in this article. Part I contains analysis on compliance tips for the advertising activities related to medical health Apps based on the attributes of medical health Apps, and Part II focuses on the personal information collection and use of medical health Apps.

## Part II

## I. Attributes of Medical Health Data

Medical health data comes from a variety of sources, including medical record information, genetic medical history, health status, medical insurance information, real-time physique index, diet structure, exercise preferences. Clarifying the legal attributes of such data is a prerequisite for the legitimate collection, use and processing. We summarize the legal definitions of common medical health data as follows:

### 1. Personal Information / Personal Sensitive Information – *Cybersecurity Law*

In accordance with the *Cybersecurity Law* and the *Information Security Technology—Personal Information Security Specifications* (hereinafter referred to as the "Specifications"), medical health data that can point to the identity of a natural person are deemed as "personal information" unless

such data are anonymized. Therefore, identity information entered by users of the App for registration, medical records, and various physiological characteristics are all information that can identify individuals. According to Section 3.2 and Appendix B of the Specifications, personal property information (e.g. users' transaction and consumption records, bank account number), personal health and physiological information, personal biometric information (e.g. Apps may collect facial information for online consultation), personal identification information, network identification information (e.g. account number, password), are "personal sensitive information" and therefore are supposed to be specially protected by law.

2. **Population Health Information** - ***Measures for the Administration of Population Health Information (Tentative)***

"Population Health Information (PHI)" refers to basic population information and medical and health service information generated in the service and administration process of medical, health and family planning service agencies at various levels. Electronic information has the same legal effect as the paper text information. It should be noted that although the responsible entities are medical, health and family planning services, such services may entrust other institutions to manage population health information, who shall therefore be responsible for PHI security and management. Apps that function as online registrants for medical services may collect and manage PHI and thus must undertake corresponding responsibilities.

3. **Human Genetic Resources** - ***Administrative Regulations on Human Genetic Resources***

"Human Genetic Resources Information" refers to information materials such as data generated from human genetic resource materials (such as organs, tissues and cells that contain hereditary substances such as human genomes and genes). Human genetic resources information that has not been anonymized may constitute personal information. Collection, preservation, use and transfer of human genetic resources information must comply with administrative approval procedures in *Administrative Regulations on Human Genetic Resources*, and must conform to ethical principles, and must respect the privacy of human genetic resource providers.

4. **Healthcare Big Data** - ***Administrative Measures on Standards, Security and Services of National Healthcare Big Data (Tentative)*** **(the "Administrative Measures")**

"Healthcare Big Data" refers to the data relating to healthcare generated in the course of disease prevention and control as well as health management. According to this definition, almost all the data collected and processed by medical health Apps constitutes healthcare big data. All types and levels of medical and health institutions and related enterprises are responsible for the healthcare big data security and application management. The responsible entity shall perform the healthcare big data management duties in accordance with the Administrative Measures.

5. **Medical Device Related Data - *Guiding Principles for the Technical Review of Medical Device Cybersecurity Registration* (the "Guiding Principles")**

Medical device related data can be divided into health data and device data. "Health Data" refers to the private data indicating physical and mental health status, and involves patient privacy information. "Device Data" refers to data describing the device operating status which is used to monitor and control the device operation or to maintain the device, and does not involve patient privacy information. For medical health Apps that constitute medical devices, operators should follow the requirements of the Guiding Principles in order to ensure the cybersecurity of medical device and maintain the confidentiality, integrity, and availability of medical device related data.

6. **Important Data - *Information Security Technology—Guidelines for Security Assessment of Data Cross-border Transfer (Exposure Draft)***

"Important Data" refers to data that directly affects national security, economic security, social stability, public health and safety, such as undisclosed government information, large-area population, genetic health, geography, and mineral resources, which can reflect population health, epidemic situation of certain areas. If medical health information collected by Apps affects public health and security, it falls within the scope of important data.

In addition, Appendix A of *Information Security Technology—Guidelines for Security Assessment of Data Cross-border Transfer (Exposure Draft)* provides a detailed list of important data of population health, which includes (1) personal privacy, patient and reporter's information, which is obtained during the reporting and monitoring process of adverse reactions in drugs and contraceptives; (2) personal privacy and related diseases, epidemiological information of patients with infectious diseases and their families, close contacts, which is obtained during public health emergencies and infectious disease surveillance; (3) personal medical records, health records, and other medical information and health data information kept by medical institutions and health management service organizations; (4) personal information of human organ donors, recipients of human organ transplant, and applicants for human organ transplant surgery; (5) personal information related to sperm and egg donors, users, applicants in human assisted reproductive technology services; (6) personal privacy involved in family planning services; (7) genetic information of individuals and families.

## II. User Information and Privacy Protection

In dealing with App's unlawful collection and use of personal information, the supervisory authorities are paying more attention to ex ante supervision and are escalating penalties. On January 25, 2019, the Cyberspace Affairs Commission, Ministry of Industry and Information Technology, Ministry of Public Security and State Administration of Market Regulation jointly issued the *Announcement on Special Operations against Unlawful Collection and Use of Personal Information through App* (hereinafter referred to as the "Announcement"). The Announcement emphasizes the principles regarding collection and use of

personal information provided in the *Cybersecurity Law* and other relevant laws, the responsibilities of respective government authorities in cracking down on personal information violations. The Announcement initiates an assessment for unlawful collection and use of personal information to be conducted jointly by the National Information Security Standardization Technical Committee, China Consumer Association, China Internet Association and China Cyberspace Security Association (collectively as the "App Special Taskforce"). The App Special Taskforce issued ***Guidelines on Self-Assessment for App's Unlawful Collection and Use of Personal Information*** (the "App Assessment Guidelines"), which aims to guiding App operators from three major aspects: privacy policy, App's collection of personal information and user rights protection. After that, the App Special Taskforce released the ***Identification Method for App's Unlawful Collection and Use of Personal Information*** (the "App Identification Method"), which lists various common personal information violations by Apps. Besides this, the National Information Security Standardization Technical Committee released ***Information Security Technology—Basic Specifications for Collecting Personal Information of Mobile Internet Applications (Apps) (Exposure Draft)*** (the "App Basic Specifications") on January 20, 2020, which lists the management and technical requirements for App's collection of personal information. In its appendix, the App Basic Specifications particularly list the minimum information and authorization scope allowed for each type of twenty-one Apps of common services.

To sum up, to comply with the requirements of relevant regulations and regulatory documents such as the Specifications, medical health Apps should improve user information and privacy protection from the following aspects:

1. Improve privacy policy.

    - Considering that App users may include disadvantaged groups such as patients with physical defects or elderly people, privacy policy should be composed in a concise and user-friendly manner.
    - Tables and charts could be used to facilitate demonstration.
    - Use enhanced notice which contains the core contents regarding collection of personal information before installation, registration, and first use by users.
    - Be User-oriented and provide "one-stop" authorization withdrawal and closure, online access, correction and deletion of user personal information, online cancellation of accounts and other functions.
    - Distinguish between core functions and peripheral functions for users to make their decisions, and inform the necessary sensitive personal information collected for the core functions.

2. Obtain informed consent.

    - Where collecting sensitive personal information, ensure that the explicit consent of the user has been obtained.
    - The user should not be required to accept and authorize multiple business functions to collect

personal information at one time by bundling these business functions of the App.

- Do not use implied consent and user's initiative to fill in, click or check as the pre-condition for activating business function or personal information collection of the product or service.
- To collect personal sensitive information, it is advisable to allow users to choose whether to provide or agree to automatically collect personal sensitive information piece by piece. When collecting personal information from trial subjects, relevant regulations regarding subject's informed consent and the collection and use of clinical research data should be followed.

3. Avoid excessive collection.

- "Minimization requirements" proposed in Section 5.2 of the Specifications must be strictly followed. To be precise, the types of personal information collected should be directly related to the realization of the business functions of the product or service.
- The frequency of automatic collection of personal information should be minimum necessary to fulfil the business function of the product or service; and the amount of personal information indirectly obtained should be minimum necessary to fulfil the business functions of the product or service.

Beware of the minimum information permitted for collection for various services by each industry as listed in the "App Basic Specifications". For example,

| Type | Personal Information | Use Requirements / Legal Basis |
|---|---|---|
| Apps for Registration and diagnosis | Web access log information | To meet relevant legal and regulatory requirements such as the *Cybersecurity Law,* and to safeguard cybersecurity. Normally, it includes IP address, user login time, user logout time, etc., and does not refer to user operation logs. |
| | Phone number | *Regulations for the Administration of Mobile Internet Application Information Services* |
| | Transaction information | *E-commerce Law*<br>*Administrative Measures on Online Transactions* |
| | Account information: account number, password | To identify registered users and to safeguard account information security |
| | Patient identification information | To authenticate the user's identity for registration appointment |
| | Doctor-patient communication information: gender, age, disease description, medical | To judge the patient's condition during online consultation by doctors |

| | | |
|---|---|---|
| | history, first-time patient | |
| | Online registration: clinical department | To complete registration for patients |
| | Third-party payment information | To pay for the registration when users using third-party payment, which usually includes the time, amount, and channel of the payment |

4. Inform users of automatic data collection tools.

   - If users' online activity information is collected by automatic collection tools during the use of the App or its background operation, App operators must ensure that collection of such information is made moderately, and must confine such information to the scope and purpose as agreed by the users.
   - App operators must include a detailed description of the technical mechanism in its privacy policy, explain the purpose of adoption of automatic tools to collect personal information, and provide to users the methods and detailed guide to restrict data collection by automatic tools.

5. Strictly check and manage third parties related to the services provided by the App, such as data processing service providers, cloud service providers; regularly check data collection and storage by accessing parties such as SDKs and APIs to ensure the security of user information.

6. If the medical data is shared from medical and health institutions, a firewall for patient data protection must be set up. Take effective desensitization measures to ensure that the data collected cannot identify, and cannot be recovered to identify specific individuals.

7. Pay attention to the possible application of extraterritorial laws, especially the regulations which govern private information and personal sensitive information such as medical information or medical history.

## III. Localization and Cross-border Transfer of Medical Health Data

1. If the medical health information constitutes PHI, medical, health and family planning service agencies at all levels shall not store such data on overseas servers, and shall not host or lease the servers outside of China. Although enterprises and individuals that use population health information or provide technical maintenance and support for population health information are not the responsible entities defined under the *Measures for the Administration of Population Health Information*, they still need to abide by these restrictive provisions.

2. If medical health information constitutes human genetic resources information, foreign organizations, individuals and institutions established or actually controlled by them may not possess such

information. If human genetic resources information must be provided, it shall be filed or recorded with the authorities in accordance with regulations.

3. If medical health information constitutes important data, the information generated during onshore business operation must be stored within China. If it is truly necessary to provide such information abroad, the operator shall conduct a security assessment. Therefore, relevant operators need to first determine whether they are critical information infrastructure operators. If so, the personal information and important data collected or generated by them must be stored within China.

4. In addition to the requirements to domestic institutions being the data transferor, the national standard *Health Information Science—Data Protection Guide to Promote Cross-border Transfer of Personal Health Information* imposes requirements on data recipients. When the data controller transfers medical data to another country, it is necessary to ensure that the data recipient takes organizational and technical security measures to fully protect the data transferred.

In short, if the App operator cannot determine whether the cross-border transfer of data (such as to overseas parent companies, affiliates or third-party data processing service providers) poses a threat to China's national security, national economy and people's livelihood and the public interest, it is advisable to conduct an ex-ante assessment to avoid blindly transferring sensitive medical health data overseas.

## IV. Data Security of Medical Health Apps

Medical health data, especially patient's data, is of important scientific and economic value. Corresponding to its high-value characteristics, the overall cybersecurity risk level of the healthcare industry is usually graded as "relatively high". The mobile internet security is of paramount importance. According to the *2019 Security Observation Report of Mobile Apps in the Health and Medical Industry* released by the China Academy of Information and Communications Technology, the security risks of medical health Apps exist in four major aspects: first, high risk of security breach; second, potential harm of malicious programs; third, third-party SDKs causing risks; fourth, relatively low rate of security reinforcement adoption. Specifically, the vulnerability of incomplete laws and regulations and standard system related to cybersecurity of mobile Apps can easily be exploited by criminals; unstandardized development processes, and delayed updates and repairs of some Apps are prominent; App users' lack of mobile cybersecurity awareness, and their bad using habits will also bring security problems.

To address the problems of App data security and reduce legal risks, operators may put it as a top priority to implement the cybersecurity graded protection (also known as "MLPS") obligations stipulated in the *Cybersecurity Law*. In fact, the Ministry of Health issued the *Guiding Opinions on the Classified Protection of Information Security in the Healthcare Industry* in 2011, which required that the healthcare industry must conduct a comprehensive graded protection of information security such as grading and record filing, construction and rectification, and assessment. Referring to the identification guidance for Critical Information Infrastructure of the *National Cybersecurity Inspection Operation Guide*, "the operation of hospitals and other health institutions, disease control, and operation of emergency centers" in the

"healthcare industry" was identified as a critical business. Entities and institutions in the field of healthcare sector are also included in the scope of critical information infrastructure protection in the *Regulations for the Security Protection of Critical Information Infrastructure (Exposure Draft)* issued in 2017. Because the *Cybersecurity Law* officially prescribed the cybersecurity graded protection system as a statutory obligation, and stressed higher level protection for "critical information infrastructure", business operators in the healthcare industry (including operators of medical health Apps) in general should consider strictly implementing the graded protection system to safeguard data security.

To be specific, App operators shall refer to *Information Security Technology - Baseline for Cybersecurity Classified Protection* to implement the following cybersecurity protection measures:

1. Complete grading, assessment and record filing, and implement cybersecurity graded protection system. Please note that "grading and record filing" and assessment are two separate procedures. Graded protection implementation does not end with grading and record filing.

2. Adopt internal security policies and operation procedures, designate persons in charge of cybersecurity, and implement cybersecurity protection responsibility system.

3. Take technical measures to prevent actions that may harm cybersecurity, such as computer virus, cyber-attack and network intrusion.

4. Take technical measures to monitor and record network operation status and network security incidents, and retain relevant network logs for at least six months.

5. Take measures such as data classification, important data back-up and encryption.

Commonly, Apps use third-party codes and plug-ins such as SDKs and APIs to assist in data collection, transfer and processing. However, such codes or plug-ins normally do not inform users when they collect data, while it would be difficult for users to detect the act of collection by themselves. Even some App operators do not know what information is collected. According to the *Information Security Technology - Basic Specifications for Collecting Personal Information by Mobile Internet Application (App) (Exposure Draft)*, the App operator shall be responsible for the collection of personal information by third-party codes and plug-ins used in such App. The personal information collected by third-party codes and plug-ins is deemed to be collected by the App. Therefore, the App operator should prevent third-party codes and plug-ins from collecting irrelevant personal information. In contrast, if the third-party codes or plug-ins explicitly inform users of the purpose, method, and scope of collection and use of personal information, and obtain prior consent, operators of such codes or plug-ins independently will undertake responsibility for their own collection. In summary, App operators should use third-party codes and plug-ins carefully, such as API interfaces. It is advisable to clarify their respective security interface and responsibilities, in contracts or in other forms, and to clearly inform the personal information subject of the third-party codes and plug-ins.

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

**David Pan**
+86 21 3135 8701
david.pan@llinkslaw.com

**For any further questions on this subject or other business consultation, please feel free to contact us: master@llinkslaw.com**

| SHANGHAI | BEIJING | HONG KONG | LONDON |
|---|---|---|---|
| T: +86 21 3135 8666<br>F: +86 21 3135 8600 | T: +86 10 8519 2266<br>F: +86 10 8519 2929 | T: +852 2592 1978<br>F: +852 2868 0883 | T: +44 (0)20 3283 4337<br>D: +44 (0)20 3283 4323 |

www.llinkslaw.com

Wechat: LlinksLaw

**WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD**