Legal Regulatory Difficulties and Countermeasures for Health and Medical Data Sharing

Hui Feng[1] Liuyang Jian[2] Honglin Zhu[3] Yuqing Zhang[4]

[1] *Renmin Hospital of Wuhan University, Wuhan, Hubei, China*
[2,3,4] *College of Humanities, Hubei University of Chinese Medicine, Wuhan, Hubei, China*
[4] *Health and Traditional Chinese Medicine Legal Research Center, Hubei University of Chinese Medicine, Wuhan, Hubei, China*
[4]*Corresponding author.*

ABSTRACT
Currently, China's medical informatization construction has entered the fast lane, and the application of health and medical data has already broken through the diagnosis and treatment process, which is closely related to the entire health system. The demand for cross-department and cross-system data circulation is becoming increasingly prominent. More people realize that health and medical data can only achieve its public value through circulation and sharing. There are still many problems in the current sharing of health and medical data in China, including the protection of usage rights and data ownership, patient privacy and informed consent rights, information standards and sharing processes. This paper analyzes the legal regulatory difficulties of health and medical data sharing in China, and proposes suggestions such as clarifying data ownership, standardizing sharing processes, adopting dynamic consent systems, and unifying information standards, providing a standardized approach for the security and compliance of health and medical data sharing.

Keywords: *Health and medical data, Data sharing, Shared process.*

1. INTRODUCTION

The sharing and openness of health and medical big data has become a common consensus among countries around the world, and the degree of data sharing can reflect the level of information development of a country or region. At present, the sharing of health and medical data in China is still in its early stages, with low efficiency, limited scope of sharing, and insufficient exploration of data value. In the process of data sharing, it still faces numerous challenges beyond technology. It is urgent to strengthen legal regulation and supervision of health and medical data.

2. OVERVIEW OF HEALTH AND MEDICAL DATA SHARING

Big data refers not only to quantitative data, but also to the intersection and flow of data. "The core essence of big data lies in sharing". Health and medical data can only maximize its value if it is accumulated into a big data collection through openness, integration, and sharing.

2.1 Concept and Characteristics of Health and Medical Data

Health and medical data is also known as medical and health big data or health big data. The National Health and Medical Big Data Standards, Safety and Service Management Measures (Trial) point out that health and medical big data is data related to health and medical care generated in the process of disease prevention and health management. Health and medical data has the characteristics of volume, variety, velocity, variability, veracity, and value. Due to the particularity of the medical industry, health and medical data has also shown characteristics of security, privacy, heterogeneity, timeliness, and professionalism in the development of medical informatization.

2.2 Concept and Model of Health and Medical Data Sharing

2.2.1 Concept

The Open Data Institute in the UK points out that data sharing refers to the activity of sharing data with specific individuals or groups under specific and controlled conditions, and is the regular and systematic sharing of data between organizations, either in one direction or for a predetermined purpose. Wang Liming believes that "Data sharing is a contractual relationship formed between the original data collector and the sharer by sharing their collected data with others." The use of data by users doesn't affect the simultaneous processing of data by enterprises, and is a typical shared resource. Health and medical data sharing refers to the act of data controllers providing their collected or processed data to a third party through transactions, exchanges, and other means, so that the third party can use the data.

2.2.2 Model

According to different sharing entities and methods, health and medical data sharing can be divided into four models: bilateral sharing, multilateral sharing, public access sharing, and controlled access sharing. The bilateral and multilateral sharing models are applicable to the flow and use of medical data between individuals, government departments, medical institutions, healthcare research institutions, healthcare enterprises, and insurance companies, among other bilateral or multilateral entities. The difference between public access sharing model and controlled access sharing model lies in the open domain of sensitive data - the public access sharing is unconditional and has a public welfare nature.

3. OVERSEAS LEGAL REGULATIONS ON HEALTH AND MEDICAL DATA SHARING

3.1 EU

In May 2022, the European Commission issued the European Health Data Space Regulations for cross-border access and sharing of health data within the EU. The regulations mainly have the following provisions on health data sharing: (1) Patients can access their electronic health data for free through cross-border digital infrastructure established by member states, and patients are allowed to share their health data with healthcare providers. When patients are in another hospital, they are not hindered by previous healthcare providers or manufacturers. (2) In cases involving significant interests, member states will be required to provide priority categories of data in a universal European electronic health record exchange format, such as patient summaries, electronic prescriptions, electronic pharmacies, medical images, and image reports. (3) All member states are required to join cross-border digital infrastructure to exchange health data for healthcare services, and must establish a digital health management agency to ensure that individual additional rights are appropriately implemented.

3.2 The US

The US Health Insurance Portability and Accountability Act (HIPAA) and its supplemental laws have become a relatively comprehensive, systematic, and highly operational specialized law for the protection of health and medical information. The HIPAA provides detailed provisions on the definition, scope, responsibilities, and other details of relevant entities in the process of sharing and opening up health and medical information. This act allows for the provision and promotion of the flow of health information necessary for high-quality healthcare, stipulates that organizations must take specific actions to protect identifiable personal health information, and establishes standards for the physical storage and maintenance of protected health information, transmission and access requirements, as well as legal usage and disclosure methods.

3.3 Japan

Japan has adopted a dual-track system of "basic law + specialized law" for the use of medical data, with the basic law being the Personal Information Protection Law and the specialized law being the Next Generation Medical Basic Law of May 2018. The implementation of the specialized law has opened up a development path for the innovation of specific data, achieving "a combination of decentralization and management". This law is divided into 7 chapters and 50 articles (excluding supplementary provisions). Chapter 3 stipulates the relevant access permits for producers of anonymous processing medical information at the administrative law level, the rights and obligations of producers of anonymous processing medical information, and the rights and obligations of

relevant practitioners entrusted by producers of anonymous processing medical information. Chapter 4 specifies specific regulations for medical information processing operators to provide medical information to medical information producers.

3.4 Russia

The Basic Principles of Citizen Health Protection Law, which came into effect in November 2011, is the "basic law" of health in Russia, covering various aspects of medical and health management. Russia doesn't adopt the method of formulating specialized laws, but fully utilizes the legal management function of basic health laws in the confidentiality and open utilization of medical and health big data. The conditions for the open utilization of medical data that need to be involved are explained in the Medical Secrets under the chapter Basic Principles of Health Protection. Article 13 of this chapter specifies that the data scope restricted by the law is "health and diagnostic information obtained during medical examinations and treatments". In addition, the 8th item of the 4th paragraph introduces the Personal Information Protection Law, which applies both the conditions of basic health laws as well as "when medical institutions exchange information, including information stored in medical information systems, they need to simultaneously consider the requirements of Russian Federation law for personal data processing".

4. THE DIFFICULTIES OF LEGAL REGULATIONS ON HEALTH AND MEDICAL DATA SHARING IN CHINA

At present, the key to hindering the sharing of health and medical data lies in the lack of basic principles and elements of data sharing, especially unclear rules on rights, responsibilities, and benefit allocation. In terms of motivation, due to the difficulty in immediately reflecting the benefits of sharing health and medical data in a short period of time, it is difficult for all parties involved, especially individuals (patients), to reflect their benefits and gains in the sharing behavior. Finally, it is difficult to ensure the security risk control of health and medical data sharing, especially with the increasing uncontrollability of privacy risks due to technological development.

4.1 Unclear Data Ownership and Ambiguous Division of Responsible Subjects

4.1.1 Unclear Data Ownership

At present, there is no consensus between academia and practice circle on the rights and attributes of health and medical data, which seriously restricts the sharing and utilization of health and medical data among relevant parties and poses great challenges to the protection of patient personal information. During the sharing of health and medical data, there are multiple stakeholders involved in multiple rights (such as the right to information, ownership, and right to earnings). Medical institutions, institutional investors, and researchers of medical data are all striving to enhance their competitive advantages in order to gain control over health and medical data. The complexity of the data ecosystem leads to the challenge of dynamic value ownership allocation in the sharing process of health and medical data. Therefore, to promote the sharing of health and medical data, one should first discuss the issue of data ownership.

4.1.2 Ambiguous Division of Responsible Subjects

At present, there is no specialized legislation on health and medical data in China, which is mainly based on administrative regulations, normative documents, and recommended standards. The overall level of legislation is relatively low, lacking comprehensive, detailed, and clear guidance and regulations, which is clearly lagging behind the current demand for the rapid development of health and medical data in the construction of "Healthy China" and "Digital China". There are not many operational rules regarding the rights, obligations, and responsibilities of all parties involved in the production, collection, use, sharing, and exchange of health and medical data. Some regulations exist in normative documents at lower levels and lack legal enforcement. The rights and obligations of legitimate users of health and medical data are not clearly defined, and the control and supervision are insufficient. There is no clear provision for specific usage permissions and it is difficult to obtain evidence afterwards, making it difficult to trace back to a specific link and determine ascription of responsibility. The existing laws are no longer able to effectively regulate the infringement of health

and medical data, which is also one of the causes of the phenomenon of "isolated data island".

4.2 Non-standardized Sharing Process Leads to Privacy Leakage

As an important factor of production and social wealth in the information age, data's nonexcludability and non-consumerism provide technological possibilities for circulation and sharing. At the same time, the constant and ubiquitous data collection and sharing behavior can also lead to the risk of privacy leakage. A medical industry data security report in the US shows that there were a total of 572 publicly disclosed medical data breaches in 2019, resulting in over 40 million patients having their private health data stolen by hackers. A US company specializing in cybersecurity services conducted in-depth research on the security of image storage and network servers and found that over a billion confidential medical images containing patient names, date of birth, examination reasons, and ID card details were exposed in public network areas, even including information about US military personnel. Massive health and medical data is generated in health and medical service activities, and if it is not properly protected during the sharing stage, it is likely to be reprocessed by the collector or shared with other entities without the consent of the patient, resulting in the continuous expansion of the transmission and use scope of health and medical data. How to balance privacy protection and data sharing has become one of the key issues in solving data sharing.

4.3 Insufficient Notification of Informed Consent

Generally speaking, data collectors and controllers are not allowed to engage in data sharing without the consent of healthcare data subjects. The reasons are as follows. Firstly, informed consent is a manifestation of the data subject's control over personal data and a concrete manifestation of information self-determination. Secondly, health and medical data contains personal information, which belongs to the category of personality rights and has exclusive attributes. No organization or individual can freely share personal information. Thirdly, it is necessary to ensure that data subjects have control over the entire process of data circulation. Data sharing is essentially the sharing of information, the flow of information, and the chain of this process may be very long, which is highly likely to be open to the public. Therefore, it is necessary to effectively ensure individuals' control over their information. In practice, relevant parties often weaken the protection of user personal information in order to pursue efficiency, especially in the legal relationship of health and medical data sharing, where there is a risk of the informed consent rule being ignored.

According to Articles 1033 and 1034 of the Civil Code, as well as Articles 14 and 29 of the Personal Information Protection Law, both general personal information and sensitive personal information should obtain the explicit consent of the information subject before processing, and the processing of sensitive personal information should also obtain the "separate consent" of the information subject. However, big data mining and analysis technologies not only make it difficult for information processors to develop complete and clear data sharing informed consent agreements, but also lead to information subjects being unable to substantially understand informed consent agreements and achieve true and "clear" "consent". In addition, health and medical data sharing is not limited to specific purposes and often adjusts with changes in scenarios, situations, and other factors. It is difficult to require information processors to fully explain the potential data utilization purposes in the future sharing process before the first processing of health and medical data information, and "Forcing information processors to inform each change in processing purposes will infinitely increase legal compliance costs."

The characteristics of secondary utilization of data and multi-link circulation also limit the effectiveness of the principle of informed consent. For users, if the medical data must be collected or used with their consent, it will increase the legal cost of using the data. In order to ensure the legitimacy of data collection, the privacy clauses of the collecting party often appear in the form of standard clauses, and users rarely actually read such clauses in the actual operation process, greatly reducing the probability of being informed. Even if users have read these privacy clauses, they may not necessarily be able to make reasonable predictions. The reason behind this is that the data involved in big data is a type of mixed data, and there is no necessary connection between the personal medical information contained in it and the processing results. In the initial stage of information collection, it is difficult for people to predict what usage the data will have.

4.4 Inconsistent Information Standards

The heterogeneity of health and medical data has led to massive data accumulation and redundancy within the system. Due to the different definitions of terms, concepts, and data types among different systems, there is a lack of unique identification for the core data entities in the diagnosis and treatment process. A large amount of health and medical data stored in unstructured forms such as text, pictures, and images can't be updated in real-time, making it difficult to fully integrate hospital information systems. Meanwhile, due to the independent procurement of information systems by major hospitals, different suppliers use inconsistent data interfaces and formats, resulting in system incompatibility, duplicate metadata collection, and uneven data granularity, making it very difficult for medical institutions to share and exchange data.

5. THE STANDARDIZED APPROACHES FOR HEALTH AND MEDICAL DATA SHARING

At present, the sharing of health and medical data in China is mostly limited to organizations such as the government, medical institutions, and research institutions, and has not yet formed principles, norms, and standards for open sharing for professional institutions and teams. The formulation and improvement of relevant laws and regulations should be accelerated to ensure the sharing and analysis of data.

5.1 Clarifying Data Ownership and Assigning Responsible Subjects

5.1.1 Clarifying Data Attributes and Attribution of Rights

Unclear data ownership not only hinders the exchange and sharing of health information, but also makes it difficult for accountability for data breaches. There are six main views on the ownership of health and medical data, namely, "individual ownership theory", "medical institution ownership theory", "individual and medical institution co-ownership theory", "public ownership theory", "composite rights theory", and "data controller rights theory". The authors believe that health and medical data is a carrier of patient personal information, which not only has property rights, personality rights, but also national sovereignty attributes.

It is recommended to clarify the ownership of rights at the legal level for the three types of stakeholders involved in health and medical data - patients, medical institutions, and the general public. Firstly, it is necessary to recognize the right of patients as information subjects to share benefits in their health and medical data, in order to encourage patients to provide their health information. Secondly, it is needed to recognize that medical institutions and related industry entities have property rights to the medical data they generate, and clarify their social responsibilities and obligations. After medical institutions collect and form data about patients during the diagnosis and treatment process, the data is separated from the patients and becomes a set of "pure data", which is stored in the medical institution's database and belongs to the medical institution, serving the diagnosis and treatment activities of patients. Finally, it is necessary to establish the public interest in health and medical data. It is important to clarify that government departments only have the right to collect and access health and medical data from medical institutions for specific purposes and under specific circumstances, with the limit of meeting the public interest.

5.1.2 Clarifying Responsible Subjects

The sharing of health and medical data activities can't be separated from multiple links such as collection, processing, utilization, and supervision. To clarify the Responsible subjects, it is necessary to sort out the main bodies of each link from the perspective of technical logic, identify the key elements that have an impact on legal relationships, and construct a "rights-obligations-responsibilities" system in the field of medical health. Under this system, patients and medical institutions are the sample subjects and collection subjects respectively, with system suppliers, data analysis companies, and technology research and development providers serving as processing subjects. Multiple entities such as the government, enterprises, and research institutions utilize health and medical data, while the health administrative department bears the responsibility of supervision and management. In the process of sharing health and medical data, data owners have the right to data, the entities processing and utilizing health and medical data bear the obligation to maintain patient privacy and health information security, and at the same time, they also need to fulfill the obligation to protect patient personal information. If they violate relevant laws and regulations, they shall bear

corresponding civil, administrative, and criminal responsibilities. When formulating the principle of responsibility, it is crucial to consider the balance of interests among all parties involved in the process of medical data sharing. The accountability procedure should also clarify the relative roles of technical developers and clinical doctors. Other manufacturers, medical equipment manufacturers, and institutional investors also need to clarify their responsibilities.

5.2 Standardizing the Sharing Process and Protecting Personal Privacy

5.2.1 Establishing a Health and Medical Data Sharing Platform

On the basis of learning from the government resource catalog systems of the US, the United Kingdom, Australia, and Japan, it is necessary to build a health and medical data resource catalog management system in China. A regional medical quality control system needs to be established, so as to integrate data centers, exchange platforms, and interface platforms, establish a shareable and real-time updated health and medical data information database, realize information exchange and sharing among medical institutions, and manage medical and health services.

The medical quality control system of this sharing platform integrates electronic medical record systems and regional medical information systems by collecting basic information of medical institutions, medical equipment information, laboratory inspection information, etc., which can comprehensively analyze and evaluate patient information and electronic medical records between hospitals, effectively controlling the behavior of medical institutions and medical personnel. At the same time, it can balance user registration and user permission management, providing a secure data transmission channel for information exchange between different medical institutions across regions, and ensuring data security and integrity. In practical operation, the system will add electronic signature items for medical workers and patients in electronic medical records. The hospital information management system, electronic medical record system, clinical information management system, electronic pharmaceutical affair management system, and clinical laboratory services combine electronic signatures with electronic authentication services to ensure the authenticity of the patient's identity, ensure the security of the patient's informed consent, prescription, etc., and ensure the legality and compliance of medical behavior.

5.2.2 Standardizing the Sharing Process

The most crucial issue in data sharing is the extent to which data controllers can share data while fully respecting the rights of data subjects. The protection of privacy should be understood in specific information flow scenarios to achieve "situational fairness", rather than defining a fixed boundary for privacy or personal information rights.

5.2.2.1 Preparation Stage for Sharing

Relevant parties can refer to Japan's national recognition system to clarify the qualification standards for anonymous processing of medical information producers and users. Operators who are recognized and allowed to process medical information anonymously are recognized as anonymous processing medical information producers. Medical institutions, governments, enterprises, and other entities can access the health and medical data sharing platform for operations within their authority after passing the national standard qualification certification. The data demander needs to submit an application for health and medical data sharing, and clarify the type and specific content of the required health and medical data, as well as the scope, mode and purpose of this data sharing. After ensuring that the network security protection level is qualified, the data shall be uploaded to the data center of the platform for review. The data center will conduct a detailed review of the legality and necessity of the content of the application form, and refuse any application forms that do not meet the requirements.

5.2.2.2 Implementation Process of Sharing

After the application form for health and medical data sharing is reviewed and confirmed to be correct, if the corresponding data has been stored in the platform database, it will be directly sent to the demander in the form of a file. If this type of data is missing in the database, the application form will be submitted to the relevant data provider port. The provider then performs de-identification processing on the data after obtaining the patient's informed consent. When patients raise objections, the provider will adjust the scope of sharing, obtain the patient's consent again, and then proceed with data sharing according to the process. The

processed data will be uploaded to the shared platform and sent by the data center to the demand side. Patients have the right to evaluate the user's usage rights, and for those who can't meet the requirements, the rights holder can call for cessation of use at any time.

5.2.2.3 *Termination Stage of Sharing*

After the end of a single sharing behavior, the platform will destroy or retain the shared health and medical data based on the patient informed consent form submitted by the data provider. The authorized sustainable sharing health and medical data will be collected and stored, a shared data directory will be created, and integrated system management will be carried out to ensure that the quality of medical data meets the standards of authenticity, accuracy, and availability. At the same time, the platform will sign a confidentiality agreement with the data demander to ensure the privacy and security of the data. Subsequently, the platform will also regularly review the qualifications of its members and optimize the sharing plan based on user evaluations.

5.2.3 *Introducing Third-party Supervisory Agencies*

Health and medical data involves sensitive information such as personal genetic information, disease history, drug history, family history, etc. Privacy security is the insurmountable warning line in China's health and medical data sharing. To achieve effective utilization of health and medical data, there must be both technical guarantees and numerous standardized standards and professional personnel to supervise and guide. At the same time as legislative protection, third-party supervisory agencies can be introduced to supervise the entire process of medical data sharing and collaboration platforms, achieving fairness, impartiality, and openness in the supervision of information sharing processes. Patients can check where their health and medical data is used at any time on the platform built by third-party institutions, and in this process, it is also necessary to ensure the integrity and safety of the system and optimize the system protection level in a timely manner.

5.3 *Performing Data Desensitization Processing and Using Dynamic Consent Mode*

5.3.1 *Ensuring Data Desensitization Processing*

De-identification refers to the process of technical processing of personal information without relying on other information, so that it can't be authenticated or associated. The de-identification of health and medical data can effectively solve the problem of collecting and storing a large amount of medical data, help doctors obtain clinical information faster, reduce the invasion of patient privacy, and improve hospital management efficiency and service level. The data de-identification standards in China should be differentiated based on different data types. For sensitive personal data, the de-identification requirements must meet the standard of no longer identifying individuals, completely disconnecting the connection between the data and specific objects. For data with weak correlation, as long as the identity of the data subject can't be analyzed through comparison, it can be considered as de-identification completed.

5.3.2 *Adopting Dynamic Consent Mode*

The transparency principle of the EU General Data Protection Regulation refers to the fact that data controllers should provide data subjects with the facts, processes, purposes, degrees, and rights of data collection, use, consultation, or processing in a clear, concise, and easily accessible manner, through clear language and appropriate measures. Dynamic consent refers to allowing individuals to voluntarily decide whether to give consent or give up based on informed methods, frequency, and content. In the dynamic consent mode, in the health and medical data sharing project, information subjects can agree or disagree based on their personalized choices, fully realizing autonomy of willingness. The rapid development of big data and Internet 5G technology has made the dynamic informed consent mode practical and feasible, which can overcome the drawbacks of information lag in traditional informed consent modes. Through the existing official account, applet and other platforms of medical institutions or health departments and other subjects, information processors can obtain effective consent in time and information subjects can also know relevant information in time.

5.4 Unifying Information Standards

The linkage between upper and lower level medical institutions is the basis for implementing hierarchical diagnosis and treatment, the interconnectivity of health and medical data is of utmost importance, and the prerequisite for interconnectivity is a unified standard. The Opinion on Strengthening the Construction of National Health Information Standardization System also points out the need to accelerate the standardization construction of national hospital information platforms and grassroots medical and health institution information platforms. Overseas, the US federal government has established professional technical teams to provide services for the standardization of government information. The Information Technology Standards Committee in Singapore has developed Multi-layer Cloud Security (MTCS) standards to address customer concerns about the security and confidentiality of cloud data. China can refer to and draw on the current national conditions to promote the establishment of the information standard system required for medical data sharing in China, such as basic information models, medical terminology, classification and coding of data categories, data elements and metadata, shared documents, as well as privacy and security related content.

6. CONCLUSION

The sharing of health and medical data is closely related to the protection of citizens' personal rights and interests, the development and utilization of commercial value of medical data, and the maintenance of public value. Although legislation related to health and medical data is constantly improving, it is still necessary to explore through legislation and practice regarding how to promote communication and sharing among data controllers on the basis of data compliance, and how to better leverage the role of emerging medical entities such as Internet hospitals while ensuring the security of health and medical data. Faced with numerous legal risks, strengthening top-level design, innovating collaborative platforms, proposing diversified solutions, and establishing a safe, orderly, and trustworthy health and medical data sharing ecosystem are the goals that need to be continuously pursued.

ACKNOWLEDGMENTS

Fund projects: the general project "Research on Privacy Right Protection in the Context of Medical Artificial Intelligence" (YF21-Y41) of Sichuan Health and Legal Research Center of Sichuan Provincial Key Research Base of Philosophy and Social Sciences, Hubei Provincial Key Laboratory Open Project "Exploration of Legal Issues Related to Sino-Japanese Smart Healthcare" of Renmin Hospital of Wuhan University.

REFERENCES

[1] Zhang Zehong, Xiong Jingjing. Synergy dilemma of healthcare alliances and trust-based countermeasures [J]. Chinese Journal of Hospital Administration, 2017, 33 (8): 565-568. (in Chinese)

[2] Wang Liming. Legal Protection of Personal Information: Centered on the Line between Personal Information and Privacy [J]. Modern Law Science, 2013,35 (04): 62-72. (in Chinese)

[3] Gao Fuping. Personal Information Protection: From Personal Control to Social Control [J]. Chinese Journal of Law, 2018,40 (03): 84-101. (in Chinese)

[4] Li Xianshu, Ning Shilei, Akhmetshin. Legal techniques of the utilization of medical big data in Russia and enlightenment [J]. China Health Law, 2023,31 (02): 54-59. (in Chinese)

[5] Deng Mingpan, Liu Chunlin.Rights Protection and Behavioral Regulation in Health Care Big Data Application [J].Medicine and Jurisprudence, 2019 (04): 42. (in Chinese)

[6] Hong Xinlin. Legal Protection of Citizens' Personal Medical Data in China [J]. Medicine and Jurisprudence, 2022, 14 (05): 82-88. (in Chinese)

[7] Jiang Bo, Zhang Ya'nan. Fair Use of Personal Information in the Context of Big Data [J]. SJTU Law Review, 2018, No.25 (03): 108-121. (in Chinese)

[8] Gao Fuping. An Entitlement of Clinical Data: the Legal Framework of Clinical Data Sharing [J]. Modern Law Science, 2020,42 (04): 52-68. (in Chinese)

[9] Yang Chaohui, Wang Xin, Xu Xianglan. Discussion and Classification of Medical

Health Big Data [J]. Health Economics Research, 2019,36 (03): 29-31. (in Chinese)

[10] Wang Liming. Data Sharing and Personal Information Protection [J]. Modern Law Science, 2019,41 (01): 45-57. (in Chinese)

[11] Ding Xiaodong. The Dilemma and Way out of Personal Information Private Law Protection [J]. Chinese Journal of Law, 2018,40 (06): 194-206. (in Chinese)

[12] Zhang Xinbao. From Privacy to Personal Information: Theory and Institutional Arrangement of Interest Reassessment [J]. China Legal Science, 2015, No.185 (03): 38-59. (in Chinese)

[13] Bao Xiaoli. Risks and Countermeasures to Data Sharing — Taking Online Lending Platforms for Example [J]. Journal of Shanghai University of Political Science & Law: The Rule of Law Forum, 2021,36 (05): 122-136. (in Chinese)

[14] Li Yuefeng, Hu Jianping, Tuo Bingbing, et al. Effect and Thinking of Health Information Standard Construction in China [J]. Chinese Journal of Health Informatics and Management, 2021,18 (03): 324-329. (in Chinese)