Legal Dilemmas and Mitigation of Healthcare Data Sharing

Liuyang Jian[1] Honglin Zhu[2] Qinglian Deng[3] Haicen Guo[4] Ke Huang[5] Xing Jiang[6] Siying He[7] Yuqing Zhang[8]

[1] *Law School, Central China Normal University, Wuhan, Hubei, China*
[2,3,4,5,6,7,8] *School of Medical Humanities, Hubei University of Chinese Medicine, Wuhan, Hubei, China*
[8] *Hubei Health Industry Development Research Center, Wuhan, Hubei, China*
[8]*Corresponding author. Email: zyq95@hbtcm.edu.cn*

ABSTRACT
The practical difficulties of healthcare data sharing in China are mainly reflected in the relatively lagging legislation, imbalanced conflicts between data sharing and protection, unclear rights and responsibilities, and insufficient security guarantees. It is necessary to enhance institutional improvement from the aspects of improving the legal regulatory system, coordinating conflicts with privacy rights, improving the application system of informed consent rights, clarifying data ownership, and strengthening security guarantees.

Keywords: *Healthcare data sharing, Data legislation, Privacy.*

1. INTRODUCTION

The "Healthy China 2030" planning outline clearly proposes the strategic policy of strengthening the construction of the population health information service system and the application of healthcare big data. To maximize the value of healthcare data, data sharing has become an indispensable part. At present, the healthcare data sharing in China is still in its infancy, and the network security situation in the medical industry is severe. Frequent data breaches and other incidents have raised deep concerns among the public about information security issues and revealed deficiencies in medical data management. In December 2020, the National Health Commission issued the “Notice on Deepening the ‘Five Ones’ Service Action of ‘Internet + Medical Health’”. The notice emphasizes that secondary and above hospitals should accelerate the interconnection of medical service information and business collaboration within the hospital, while promoting data sharing and business collaboration relied on physical medical institutions. In order to ensure the safety, reliability, and long-term stable development of healthcare data sharing, it is urgently necessary to strengthen legal protection.

2. HEALTHCARE DATA SHARING AND APPLICATION SCENARIOS

2.1 Concept of Healthcare Data Sharing

Data sharing originated in the field of clinical trial data for drug development, with a particular emphasis on the sharing of raw data in practice and advocacy, specifically referring to activities involving multiple stakeholders (such as researchers, government regulatory agencies, funders, and medical publishing institutions). Healthcare data sharing refers to the process of sharing and exchanging medical information and data among medical institutions, doctors, and researchers. This sharing not only helps to improve the efficiency and quality of medical services, but also promotes scientific research and innovation, providing strong support for disease prevention and public health. In addition, medical data sharing can promote global health cooperation and advance the medical industry.

2.2 Application Scenarios of Healthcare Data Sharing

China's healthcare data sharing activities tend to rely on "platforms" to promote the interconnection and sharing of health and medical data by building national, provincial, and city/county level healthcare data platforms.[1] With the construction of a hierarchical healthcare data sharing platform in China, the application scenarios are becoming increasingly broad. (As shown in “Table 1”)

Table 1. Application scenarios of healthcare data sharing

Application scenarios	Approach	Usage
Clinical diagnosis and treatment	The interconnection of clinical diagnosis and treatment information within the hospital relies on the hospital's electronic medical record system; Inter hospital reliance on regional medical information platforms	Implementing a hierarchical diagnosis and treatment system and carrying out remote medical work
Patient information acquisition	Downloading personal medical records at anytime and anywhere via the Internet. Collecting healthcare data by relying on the original clinical and public health information database of the hospital or the region or through a special open platform for scientific research data	Recording personal medical records for secondary use
Public health information sharing	The system data sharing mode focuses on the linear pattern of business processes, from the central to the grassroots platform; The data sharing model of the regional health information platform focuses on the block-based accumulation of data, gathering and sharing comprehensive and continuous data information.	Preventing and controlling the spread of epidemic diseases; Facilitating the exchange of various types of information between internal public health information systems and with district health information platforms
Administrative management decision-making	Obtaining macro management data through regional health information platforms[2]	Utilizing the application value of big data in health resource regulation, policy formulation, performance evaluation, supervision, and deep data mining and utilization
Scientific research	Collecting healthcare data through hospitals or existing clinical and public health information databases in the region, or through specialized scientific research data open platforms[2]	Completing data acquisition to provide data support for scientific research

3. BASIC FORMS OF HEALTHCARE DATA SHARING

3.1 Bilateral Sharing

Bilateral sharing is the simplest form of health data sharing, involving two entities sharing healthcare data with each other. It can occur between data subjects, data holders, and users,[3] as well as between data holders and data users, including but not limited to medical institutions, research institutions, medical insurance companies, and government agencies.

3.2 Multilateral Sharing

Multilateral sharing is the process of the flow and use of healthcare data between two or more entities. In this sharing model, there are at least two data providers (which can be data subjects or data holders) and one data user. From the perspective of sharing scope, it includes internal sharing, such as sharing between different departments within a hospital; This also includes external sharing, such as medical institutions sharing patients' medical data with both medical research institutions and government agencies to support large-scale disease research and treatment plan improvement, or to assist government agencies in public health monitoring, disease prevention and control, and policy formulation.

3.3 Public Access Sharing

Public access sharing is generally applicable to the sharing of data that is not sensitive in the public domain. Its characteristic is that the shared objects are usually non-specific general subjects (such as individuals, enterprises, medical institutions, etc.), which are unconditionally open to the outside world for sharing, and therefore often have public interest. For example, the government's health regulatory authorities open up the sharing of their health resource data and public health data.

3.4 Controlled Access Sharing

Controlled access sharing is suitable for sensitive databases, limiting access to specific industries or groups, and implementing security measures to protect data. This sharing method can

be divided into two types of centralized mode and federated mode. In centralized mode, data is stored in a central database, managed by specific institutions or organizations, and only authorized users can access the data. In the federated mode, multiple institutions collaborate to share data, which is distributed in different locations. Each institution retains ownership of the data but shares access permissions.

4. LEGAL DILEMMAS OF HEALTHCARE DATA SHARING

4.1 Relatively Lagging Legislation on Healthcare Data

At present, there is still a gap in specialized legislation in the field of healthcare data in China, and relevant regulations are mainly scattered among different levels of laws, administrative regulations, departmental rules, and local regulations, without forming a systematic collective effect. Specifically, although Articles 111 and 1034 of China's “Civil Code” have clearly stipulated that "personal information of natural persons is protected by law", the “Cybersecurity Law” further defines the scope of personal information and incorporates it into the overall protection framework of network security.

On this basis, the “Personal Information Protection Law” further absorbs the legislative essence of the “Civil Code” and the “Cybersecurity Law”, with its core focus on strengthening the protection of personal information rights. However, from a global perspective, the regulations of this law in the field of healthcare data still mostly remain at the level of framework and principles, especially in key aspects such as data collection, storage, use, and disclosure. There is still a lack of specific and actionable guidelines, which undoubtedly poses certain challenges to the security management and effective utilization of healthcare data. This has to some extent affected the actual implementation effect of the law in the field of healthcare data protection. Although the “Guidelines” provide specific requirements for the use and disclosure of healthcare data, they are recommended national standards and lack legal enforcement.

4.2 Unclear Ownership Regulations for Healthcare Data

As an important component of personal information, the ownership of healthcare data should follow the basic principles of personal information protection. The “Personal Information Protection Law” and other relevant laws and regulations provide a basic legal framework for the ownership of healthcare data, but do not clearly define the specific ownership of healthcare data. This has led to differences in ownership, usage, and revenue rights of data among various parties in practical operations, making it difficult to form unified norms and standards.

At present, there is a heated discussion in the academic community about the ownership of healthcare data. Some argue that data property rights should belong to the data processors, as the value of data needs to be reflected through processing and circulation; There are also views that data should belong to the data subject and be authorized to data controllers and users under the principle of informed consent[4]; Another viewpoint is that under a sound sharing mechanism, all parties in the healthcare data sharing chain have the right to benefit. For example, some medical institutions tend to believe that they have ownership of the data because they participate in the collection of patient data.

4.3 Conflicts Between Healthcare Data Sharing and Privacy Protection

4.3.1 Specific Manifestations of Conflicts

Firstly, there is a certain conflict between data sharing and privacy protection for self-determination. As citizens' right to personal lifestyle and decision-making, the right to self-determination privacy is facing new challenges in the Internet era. With the widespread application of healthcare data, the collection and processing of personal data may to some extent limit citizens' self-determination choices. Secondly, data sharing conflicts with spatial privacy protection[5]. The right to spatial privacy refers to the individual's right not to be violated by others in a specific private space, which applies to both physical and virtual spaces. With the development of network technology, personal spatial privacy is easily violated by hackers and virus programs, but excessive protection of spatial privacy may hinder the effective operation of data sharing. Finally, data

sharing conflicts with information privacy protection. Once personal information is leaked to the Internet, it will be difficult to recover. At the same time, because the scope of personal privacy information is vague, it is easy to make data sharing fall into an infringement storm, increasing the cost burden of data subjects.

4.3.2 Reasons of Conflicts

Firstly, there are conflicts between public interest and personal interest. In the context of smart medical care, personal privacy rights refer to the right of citizens to have their legally held personal information not disclosed or illegally infringed upon, as well as the right to control and use personal information when receiving health services. In order to ensure public health safety, health administrative departments need to accurately and reasonably collect, use, and process health data, which contradicts individuals' desire to enjoy a solitary and peaceful life in the private sphere. Secondly, there are conflicts between property interests and personal interests. Currently, many commercial companies are actively collecting and utilizing massive amounts of personal health and medical data, which undoubtedly exacerbates the risk of personal privacy infringement. Although the collection and utilization of these data have their positive aspects, they also bring potential threats to individual privacy rights. For example, companies providing wearable devices that conduct commercial operations by collecting personal health information may result in potential personal economic losses and health discrimination. In addition, there are dual interests in healthcare data. Data sharing emphasizes the protection of data property interests, while personal privacy protection focuses on the personal interests of data, leading to conflicts between data sharing and personal privacy protection.

4.4 Lack of Unified Data Masking and Anonymization Standards

Data masking is a data protection technique that uses processes such as de-identification or encryption to make it impossible to identify an individual's identity. The “Personal Information Protection Law” requires personal information processors to adopt measures such as anonymization and encryption to protect the security of personal information, but does not specify the standards and methods for anonymization. Some technical standards and guidelines provide recommendations and principles, but the specific implementation methods for anonymization still need to be decided by personal information processors themselves, resulting in limited consistency and comparability of desensitization results.

Data anonymization refers to a technical means of making data unable to be associated with individuals and cannot be restored through technological processing, in order to maintain data availability. Although regulations such as the “Cybersecurity Law” allow anonymous personal data to be provided to other citizens for use, providing a legal basis for the commercialization of anonymous big data, the rules for personal data anonymization are too general, and the scope, procedures, effectiveness, and other provisions are not clear. In addition, anonymization cannot completely prevent data restoration, and some advanced technologies and combination attacks may still identify individual identities. Therefore, caution should be exercised in handling and assessing risks, and anonymization standards should be constructed based on data application scenarios.

4.5 Insufficient Protection of Traditional Informed Consent Rights

4.5.1 Informed Consent Mechanism Becoming Mere Formality

Informed consent in healthcare data protection refers to individuals giving clear, voluntary, and informed consent to the use and processing of their own healthcare data. On the surface, it seems to fully respect the individual's information autonomy and personal dignity, but in reality, relying solely on formal informed consent documents may overlook the complexity of sharing healthcare data, leading to informed consent becoming mere formality.

Firstly, the protection of healthcare data involves professional terminology and complex regulations, making it difficult for individuals to understand the meaning and potential risks of the data. They can only hastily agree or refuse, and cannot make accurate judgments. Secondly, in some cases, the sharing entities of medical data treat informed consent only as a standardized procedure rather than a genuine mechanism for communication and discussion. Especially in the process of data sharing, as data circulation becomes increasingly complex, multiple uses with one

authorization have become the norm. If each link requires individual informed consent, the increase in data costs will lead to individuals being unwilling to pay, which can easily result in unauthorized data collection and illegal use. Finally, due to the imperfect legal system and regulatory mechanisms, sharing entities may use individual health data for other purposes without authorization, using vague terms and loopholes in the law to bypass the informed consent process, making the informed consent mechanism superficial.

4.5.2 The Detailed Provisions of the Informed Consent Mechanism Being Incomplete

To resolve the conflict between patients' healthcare data sharing and individual privacy protection, China has adopted an informed consent mechanism centered on autonomous choice, clearly defining the rights and interests of individuals as data subjects in terms of autonomous decision-making and choice. However, the relevant laws do not provide detailed regulations on the informed consent mechanism, lacking transparency and openness. There is still controversy over the validity of data subject consent for uncertain studies and situations where patient data may need to be obtained. In addition, research and public interest needs are often established as exceptions to consent, and medical institutions and related enterprises often use statutory exceptions to weaken patients' autonomy and choice. Compared to extraterritorial norms, China has adopted the principle of special law being superior to general law in expanding the scope of consent of information subjects, in addition to citing general legal provisions in the “Cybersecurity Law”. For example, in the fight against the "COVID-19" epidemic, legally authorized institutions can break the consent rules, collect the behavior tracks of patients and suspects, and conduct analysis and tracking.

4.6 Difficulties in Ensuring the Security of Healthcare Data Sharing

4.6.1 Lack of Effective Technical Protection Measures

The “2019 Healthcare Industry Network Security Observation Report” shows that the network security risks in the healthcare industry are still relatively high. In the traditional process of sharing healthcare data, the stored data is in the central database of medical institutions' servers or cloud, which poses a single point of failure risk and is vulnerable to hacker attacks and anonymous intrusions. In addition, the current Chinese medical image platform with cloud computing as the core is developing rapidly. The image cloud platform relies on the Internet to share expert resources online, which may lead to problems such as missed diagnosis and misdiagnosis of images provided by hospitals, and may easily lead to medical malpractice disputes. The serious security issues in data sharing, such as malicious cyberattacks and data breaches, highlight the urgent need to improve the security protection technologies and mechanisms required for open sharing of health record data in the digital healthcare era.

4.6.2 Industry Self-discipline Needing To Be Strengthened

There is still a lack of unified and standardized industry standards in the field of healthcare data protection, which makes it difficult for different institutions to coordinate and unify their measures in data protection, leading to many loopholes in privacy protection. At the same time, the use of personal healthcare data by medical institutions does not comply with legal and ethical principles. Each medical institution subjectively sets standards based on its own situation, which can easily lead to industry violations and fail to effectively protect the informed consent rights of data subjects. The "Investigation and Analysis Report on Personal Information Leakage in Apps" released by the China Consumers Association in 2018 revealed in detail the severe situation of current app information security. The survey results show that up to 80% of respondents have reported experiencing the dilemma of personal information leakage. The report also pointed out that 91% of applications engage in excessive collection of users' personal information, which has raised great concerns about user privacy protection. Further analysis revealed that approximately 34% of applications did not explicitly publish privacy protection terms to users, and 41% of privacy policy positions were not set prominently enough to attract users' attention. Although some platforms provide privacy policy templates, such measures often become mere formalities and fail to effectively protect user privacy. At present, the Internet health platform lacks unified assessment and evaluation standards in terms of self-regulation, which, to some extent, hinders the possibility of

conducting a comprehensive investigation and monitoring.

4.6.3 Imperfect Regulatory System

According to the “Management Measures”, the National Health Commission is responsible for establishing an open and shared mechanism for healthcare big data, and health administrative departments at all levels are responsible for supervising the security and application management of healthcare big data in their respective administrative regions. However, there are no detailed regulations on the specific supervision methods and contents. The existing supervision of healthcare data is mainly carried out by the National Health Commission, while others include the Food and Drug Administration, the Development and Reform Commission, the Ministry of Public Security, etc. In practice, there is a phenomenon of cross-functional supervision among regulatory agencies, resulting in low regulatory efficiency and increased law enforcement costs. In addition, China's regulatory system is one-way top-down supervision, lacking cooperation and division of labor among departments. Many regulatory systems lack enforcement rules, which make it difficult for regulatory authorities to take action.

5. DILEMMA MITIGATION OF HEALTHCARE DATA SHARING

5.1 Accelerating the Construction of a Legal System for Healthcare Data

5.1.1 Defining the Ownership of Healthcare Data

In the era of healthcare data sharing and application, the ownership of healthcare data belongs to individual entities. Individuals have transferred the right to use their original data in medical activities to relevant entities in the medical field, but relevant institutions, platforms, and enterprises have invested a lot of funds, technology, and labor through data collection, analysis, and utilization processes. The data results obtained should belong to these institutions. It is recommended to improve the informed consent mechanism and reasonable usage channels for healthcare data. Medical subjects should fully inform data subjects of the purpose, form, and scope of data collection, and legally obtain and use data with the consent of individual subjects.

5.1.2 Standardizing the Obligations of All Parties Involved

In the protection of healthcare data, as the first responsible person, individuals should enhance their awareness of data security, attach importance to personal information protection, regularly update security software, and actively protect their rights once information is leaked. Data processors can be organizations or individuals who independently decide on the purpose and method of processing, and they have a responsibility to ensure data security. Data processors should establish a management organization and a data security manager internally, regularly assess risks, provide feedback on results, take remedial measures, and report in a timely manner. According to the “Cybersecurity Law”, the central and local cyberspace administration departments have the responsibility to protect personal information security.[6] The government should ensure that the access information of medical industry data sharing platforms is publicly disclosed in accordance with the law, and fulfil its regulatory responsibilities for medical industry data sharing.

5.2 Clarifying the Standards for Healthcare Data Masking and Anonymization

For personal data protection, the laws of the United States and the European Union have adopted similar attitudes in regulating anonymized data, that is, data that has undergone legal anonymization processing will no longer be subject to privacy protection regulations such as GDPR and HIPAA due to its separation from personal information. This processing ensures the anonymity of the data, effectively avoiding the risk of personal privacy leakage, while also providing protection for the legitimate use of the data. The difference is that the United States' de-identification legislation is more comprehensive and operational, while the EU's anonymization rules are logically more complete and not limited to medical data. In view of this, China can learn from the experience of the European Union and the United States in the future, combine the hierarchical classification management system of healthcare data and different application scenarios, clarify the standards and requirements for health and medical data desensitization, data masking and anonymization, and establish a

personal information security risk assessment system for healthcare data, further clarifying the obligation of data holders to continuously monitor, evaluate and control risks of desensitized and anonymized healthcare data.

5.3 Refining the Classification Management Measures for Healthcare Data

It is recommended to develop and implement a hierarchical classification system based on the requirements of various policy norms such as the "Data Security Law" and the "Guidelines", with the management and utilization of healthcare scientific data throughout its lifecycle as the main line. Further refinement should be made according to the application scenarios of personal healthcare data based on the "Guidelines", and dynamic classification and grading standards should be formulated. When data processing behavior is evaluated as high-risk, data processors have the responsibility to take measures to reduce risks to ensure its continued operation. In addition, data protection measures and access authorization management are determined based on the data level. For example, privacy information needs to be desensitized, sensitive information needs to be encrypted and audited, higher-level access authorization needs to be set, and access control for basic health data can be relaxed appropriately, using techniques such as data perturbation and distortion processing to protect it.

5.4 Improving the System of Informed Consent Rights

5.4.1 Establishing a New Model of Dynamic Informed Consent

To address the issue of general informed consent, a dynamic informed consent mechanism can be established for the processing of personal healthcare data. In the process of data processing, if there are new processing directions, processing purposes, or changes in processing subjects, individual consent needs to be obtained again, and subjects have the right to withdraw from the study at any time, ensuring their right to know and decision-making. Compared to general informed consent, dynamic informed consent emphasizes that consent is a two-way and continuous interactive process between data providers and researchers, enabling researchers to make rational decisions based on their own values on the valuable information provided. This helps to maximize transparency in data utilization, enhance communication, and form consensus.

5.4.2 Diversified Ways of Making Consent

Firstly, the way of expressing actions can refer to the provisions of GDPR, including selecting options in the interactive interface, written or oral forms, etc., which can exclude default selected options and simple silence. Secondly, the implied expression of intention may refer to when the information subject is informed of a data processing policy or terms, and if they do not explicitly refuse or raise objections, it can be considered as implied consent, which does not exclude the option of default check, but still excludes pure silence. Finally, silence should not be seen as an effective form of consent, as in the field of data protection, it cannot fully reflect one's autonomous will as a pure inaction.

5.5 Strengthening the Security Guarantee of Healthcare Data Sharing

5.5.1 Improving Protection Technology Measures

In the process of transmitting healthcare data, advanced encryption transmission protocols such as SSL/TLS should be used to ensure that the data is always in an encrypted state during transmission, effectively preventing hackers from stealing and tampering. When the data enters the storage stage, symmetric or asymmetric encryption algorithms need to be used to encrypt sensitive data, ensuring absolute security of the data on the storage medium. In addition, the rise of blockchain technology has brought new perspectives and challenges to the security protection of healthcare data. Blockchain electronic medical records can encrypt and store patient personal information on the blockchain, set permissions for information, protect patient privacy data by blurring patient personal names, ages, etc., and achieve de-identification and sharing of medical data.

5.5.2 Strengthening Industry Self-discipline

The healthy and sustainable development of any industry depends on industry self-discipline. It is necessary to strengthen the supervision of medical information related enterprises and institutions,

strictly regulate the collection, processing, application, and medical research process of personal diagnosis and treatment information. At the same time, it is also necessary to establish and improve access standards, permission standards, and operational norms for personal privacy data to ensure that personal privacy data is fully protected and prevent data leakage and abuse. Industry associations should also play a role in self-discipline, formulate actionable rules, become a bridge of cooperation between data service companies and governments, and provide a positive interactive channel for formulating health industry policies and clarifying development directions.

5.5.3 Establishing a Sound Regulatory System

In terms of regulatory system, a mechanism combining government and non-governmental regulation can be established. Industry associations can lead and supervise medical organizations to comply with regulations and industry rules, and improve the level of data security protection. It is suggested to further clarify the responsibilities of regulatory entities at the organizational level and optimize organizational models to adapt to constantly changing challenges. It is also possible to consider establishing specialized regulatory agencies to build a government led and multi-level regulatory system. In addition, a system framework for pre-approval or filing should be established by introducing healthcare data sharing agreements to ensure the compliance of data sharing activities. A full process supervision mechanism should be implemented to achieve comprehensive monitoring and management of health and medical data sharing activities. A Health and Medical Data Committee should also be established in the National Health Commission, with clear responsibilities and powers, to provide a channel for public complaints about violations of personal information and privacy rights.

6. CONCLUSION

The value and life of data lies not in protection, but in its use. Healthcare data has become an important asset and source of competitiveness for medical institutions. Faced with the wave of digital transformation and the development trend of integrated medical and health systems in China, effective data governance is an important foundation for information interconnection and data value mining.[7]

ACKNOWLEDGMENTS

Fund Project: Key Research Base of Philosophy and Social Sciences in Sichuan Province — General Project of Sichuan Health Rule of Law Research Center “Research on Privacy Protection under the Background of Medical Artificial Intelligence” (YF21-Y41).

REFERENCES

[1] Zhang Jiannan, Li Yingying, Gu Yanju, et al., Discussion on the Basic Principles for Health and Medical Data Sharing [J]. Strategic Study of CAE, 2020, 22(04): 93-100.

[2] Xu Ting, Yu Guangjun, Exploration and Analysis of Application Scenarios and Value of Healthcare Big Data Sharing [J]. China Digital Medicine, 2020, 15(07): 1-3.

[3] Guan Jian, Ethical Requirements and Management Standards for the Sharing and Re-use of Scientific Data in Healthcare and Medicine (IV) Ethical Requirements: Innovative Interpretation of the Basic Ethical Principles [J]. Chinese Medical Ethics, 2020, 33(06): 645-649+683.

[4] Xu Ke, Three Approaches to Data Protection: Comment on the Case of Weibo Accusing Maimai of Unfair Competition [J]. Journal of Shanghai University (Social Sciences Edition), 2017, 34(06): 15-27.

[5] Wang Yan, Ye Ming, Conflict and Balance between Personal Data Sharing and Privacy Protection in the Era of Artificial Intelligence [J]. Journal of Socialist Theory Guide, 2019(01): 99-106.

[6] Wen Libin, Experience and Realization of Local Legislation on Personal Information Protection [J]. The South China Sea Law Journal, 2019, 3(03): 82-89.

[7] Shi Jingjin, Yu Guangjun, Governance framework and countermeasures for sharing health care data cross-regional specialty alliances [J]. Chinese Hospitals, 2023, 27(5): 43-46.