**World Journal of Sociology and Law**
**ISSN: 2960-0308**
**DOI: https://doi.org/10.61784/wjsl3005**

# LEGAL REGULATION OF PERSONAL HEALTH DATA SHARING IN THE EU AND ITS IMPLICATIONS FOR CHINA

ZhaoXia Deng
*School of English for International Business, Guangdong University of Foreign Studies, Guangzhou 510420, Guangdong, China.*
*Corresponding Email: Angelina_dzx@163.com*

**Abstract:** In practice, personal health data involves multiple subjects and diverse forms of interests, and problems such as insufficient data autonomy, privacy protection, and weak supervision have not been effectively solved, seriously hindering the development and utilization of personal health data. In view of this, this paper explores the beneficial practices of personal health data protection in the EU from legislative and practical perspectives, and proposes corresponding countermeasures to enhance China's legal protection system for personal health data, which mainly includes: (1) improving relevant legislation to fully guarantee the sharing of personal health data; (2) protecting patient privacy to safeguard the exercise of data subject rights; (3) strengthening the construction of technical standards to promote trustworthy circulation among data controllers: (4) clarifying profit rules to safeguard the legitimate interests of data processors and users.
**Keywords:** Personal health data; Sharing; EU legislation; Data controller; Technical standard

## 1 INTRODUCTION

Personal health data is a broad concept that includes “personal attribute data, health status data, medical application data, medical payment data, health resource data, public health information, etc.”[1] From clinical and health management, new drug and medical equipment research and development, to disease prevention and public health services, the types and scale of collection, use, and sharing of personal health data are more extensive than ever before.[2] “Personal health data sharing” refers to the act of the controller of personal health data providing the collected or processed health data to third parties for use without losing the right to use it.[3] The “Three Year Action Plan for Data Element X” (2024-2026) proposes the application scenarios of “Data Element X Medical Health,” requiring the orderly release of the value of health and medical data, the improvement of personal health data archives, the integration of physical examination, medical treatment, disease control and other data, and the innovation of data-driven public service models. At the same time, China has successively promulgated regulations such as the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law with the main purpose of ensuring data security, which include personal health data as sensitive personal information for strict protection. However, in practice, personal health data involves multiple subjects and diverse forms of interests, and issues such as insufficient data autonomy, weak privacy protection, and inadequate supervision have not been effectively addressed, seriously hindering the development and utilization of personal health data. In view of this, this paper, based on the legislation and practice of personal health data protection in the EU, explores the beneficial practices of personal health data protection in the EU, and attempts to propose countermeasures to enhance China's legal protection system for personal health data.

## 2 OVERVIEW OF THE LEGAL BASIS FOR PERSONAL HEALTH DATA SHARING IN THE EU

### 2.1 The Legislative Orientation of Personal Health Data Sharing in the EU

The EU takes basic human rights as the starting point for protection and emphasizes comprehensive protection of personal data through a unified legislative model. Focusing on the field of health data sharing, the current unified legislative model of the EU mainly consists of the following three landmark legal documents: firstly, the world's first international data protection convention, the Convention on the Protection of Individuals in the context of Automated Processing of Personal Data, promulgated by the European Commission in 1981; The second is the European Data Protection Directive passed in 1995; Thirdly, GDPR was promulgated in 2016. These three legal documents all revolve around how to protect personal information and privacy in the process of personal data sharing, and the restrictions on the collection, transmission, processing, distribution, and use of personal information of citizens within the EU are becoming increasingly strict; In particular, GDPR is known as the strictest data protection regulation in history, and one of its notable features is the expansion of its jurisdiction, making the strict personal data protection standards within the EU widely applicable extraterritorially. For example, Article 45 of GDPR makes the adequacy decision of data protection a prerequisite for the free flow of data, requiring EU citizens' personal data not to be transferred to countries and regions that cannot provide sufficient levels of data protection. According to Article 45 (2) of GDPR, the European Commission needs to consider three factors when assessing whether the level of data protection is sufficient: first, the rule of law, the degree of respect for human rights and freedoms; Secondly, whether there is an independent data protection regulatory agency; The third is whether to participate in international organizations or treaties related to

personal data protection. Given the strict standards of GDPR in terms of adequacy determination, currently only a few countries such as Argentina, Canada, New Zealand, Switzerland, Japan, and Uruguay have received adequacy determination from the EU.

### 2.2 Basic Provisions for Sharing Personal Health Data in the EU

There are two fundamental provisions in GDPR regarding the legal regulation of health data sharing. One is the six situations in which personal data can be legally processed as stipulated in Article 6 (1) of GDPR: obtaining the consent of the data subject; one party to the contract makes a request for the data subject or the data subject before the contract is signed; the data controller must process in order to fulfill its legal obligations; it is necessary to process in order to protect the interests of data subjects and other natural persons; processing is necessary for the public interest or for authorized data controllers to perform tasks; it is necessary to process for the legitimate interests of data controllers or other third parties. Another fundamental legal provision is Article 9 (2) of GDPR, which provides for ten exceptions to the prohibition of processing sensitive data as stipulated in Article 9 (1). It is not difficult to see from the provisions that these exceptions are based on the six categories of situations where personal data can be legally processed, involving the rights and obligations of data subjects and data controllers, as well as public interests and scientific and historical research purposes.

In addition, the EU Medical Device Regulation, the In Vitro Diagnostic Medical Device Regulation, the Artificial Intelligence Act, the Data Governance Act (proposed), the Data Act (proposed), the Network and Information Systems Security Directive, and many other applicable rules for sharing health data in the EU are also provided. For example, the Network and Information Systems Security Directive, as the first EU law related to cybersecurity, mainly includes general provisions, national frameworks for network and information system security, cross-border cooperation, and network and information system security for basic service operators and digital service providers. It aims to protect the security level of network system categories not covered by GDPR, and also applies to ensuring the security of critical infrastructure such as electricity, water supply, healthcare, and transportation industries. The security of the European Health Data Space will undoubtedly be based on this directive. Medical device software needs to be certified according to the Medical Device Regulation, and once AI based medical devices and other AI systems come into effect, they also need to comply with the requirements of the Artificial Intelligence Act.

Nevertheless, there is still a certain regulatory gap in the use of electronic health record systems in the healthcare sector. Therefore, the European Health Data Space Regulation specifically sets basic requirements for electronic health record systems to promote interoperability and data portability of such systems, enabling natural persons to more effectively control their electronic health data. For the secondary use of electronic health data, the European Health Data Space Regulation establishes a horizontal framework based on the proposed Data Governance Act and Information Act. The Data Governance Act sets general conditions for the secondary use of public sector data, but does not create real rights. The Data Act enhances the portability of certain user generated data, but does not provide rules for all health data. Therefore, the European Health Data Space Regulation supplements these proposed legislative acts and provides more specific rules for the health sector, covering the exchange of electronic health data, which may affect providers of data sharing services, ensure the format of health data portability. The cooperative rules of altruism in health data and the supplementation of obtaining private data for secondary use.

## 3 LEGAL PROTECTION STRATEGIES FOR PERSONAL HEALTH DATA SHARING IN THE EU

### 3.1 Raw Data Provider: Empowering Data Autonomy

The core feature of the EU health data space is patient autonomy. According to the European Health Data Space Regulation, patients have the following rights: (1) the right to access health data for single use immediately, free of charge, in an easily legible, summary and accessible format; (2) Electronic copies of relevant data can be obtained; (3) Users can request online modification or deletion of data, and data controllers and processors must protect the right of patients to delete their health data; (4) The right to pass on data means that the patient is entitled to pass on the medical data which he has previously received to a health care establishment for inspection by another data controller, without being prevented from doing so by the prior data controller; (5) The right to obtain information from medical professionals who have accessed their health data in the context of medical services, which should be provided free of charge through health data access services.

Regarding the principle of “informed consent,” according to GDPR, for the processing of special category data such as health data, relevant medical institutions or organizations must obtain the “explicit consent” of the data subject. The “explicit consent” here includes the following content: (1) consent must be based on the free will of the data subject and the burden of proof lies with the data controller; (2) the written declaration of the data subject not only includes the content of the consent, but also has to be clearly distinguished from other; (3) medical institutions should inform patients about the possible risks associated with collecting and processing data in an easily understandable and accessible format, in clear and concise language; (4) the processing of health data must comply with the principles of legitimate purpose, minimum necessity, and proportionality. Excessive data collection that violates these principles may result in invalid patient consent; (5) medical institutions need to inform patients of their decisions made based on automatic processing and explain the logic and implications of automatic data processing.[4]

Regarding the anonymization of data, medical institutions must comply with specific rules regarding anonymization and

pseudonymization when sharing health data, and the standard for determining whether data is pseudonymized or anonymous is recognizability. “Pseudonymization” refers to the process of processing personal health data so that specific subjects cannot be identified without additional information. Such supplementary information shall be stored separately, and technical and organizational measures shall be taken to ensure that the personal health information does not belong to an identified or identifiable individual, and data that has been pseudonymized remains personal data. Once the data is truly anonymized and unable to identify individuals, it will no longer fall within the scope of personal data protection.[5] GDPR sets a reasonable possibility standard for anonymous information. First, when determining the possibility of re identification, it should cover the data controller and any other person. Second, all reasonable and possible means should be considered, and when judging whether the means are reasonable, all objective factors should be taken into account, such as identification costs, required time, available technology at that time, and the possible development of technology.

### 3.2 Data Controller: Strengthening Data Security and Technical Standard Construction

In terms of data security. The European Health Data Space Regulation provides clear provisions on how data controllers can protect the security of health data. Firstly, implement security measures that are compatible with the risks of data utilization. In response to predictable risks that may harm patients' personal privacy, data controllers should adopt adequate technical and organizational measures to ensure that the processing is secure and consistent by means of proposed data protection and standard data protection. Secondly, promptly report the status of data breaches. Report to regulatory authorities within 72 hours from the discovery of a health and medical data breach incident, specifying the type, quantity, potential consequences, and recommended measures for handling the leaked data. The data controller should also provide a complete record of the data breach incident for regulatory agencies to verify. Thirdly, data security impact assessment. Before data controllers engage in data sharing, they should consider the nature, scope, content, and purpose of the sharing behavior, as well as the potential risks to the rights and freedoms of data subjects, and complete an assessment report on the impact of the envisioned sharing behavior on health data protection.

In terms of technical standard construction. The European Health Data Space Regulation is based on trust thinking to create a community of data interests, establish cross-border infrastructure and unified interoperability standards within the EU, and ensure that data parties can process and standardize the use of data in compliance. EU establishes European electronic cross-border health services for the one-time utilization of health data MyHealth@EU. To support cross-border sharing of health data among patients, MyHealth@EU Composed of the National Digital Health Contact Point and the Digital Health Central Platform. To promote data sharing and interoperability, the EU has established a unified European electronic health record exchange format, which allows for the transfer of electronic health data between different software applications, devices, and healthcare providers. For the secondary utilization of health data, the European Union has established a distributed infrastructure for cross-border projects HealthData@EU. Each member state should designate a secondary national contact point, which is Health-Data@EU. Each authorized participant should possess the corresponding technical capabilities to connect and participate HealthData@EU. In addition, the European Commission has established a directory of EU health datasets, connecting datasets established by national health data access agencies and authorized participants.[6] At the same time, to ensure data quality, each dataset has EU data quality and utility labels provided by the data holder, which include basic data information, technical quality, data quality management processes, coverage, etc. This will also help ensure the quality of health data in a broader sense.

### 3.3 Data Processors and Users: Clear Obligations and Profit Distribution Rules

In terms of data revenue distribution. Although the European Health Data Space Regulation does not provide a clear definition of the right to data revenue, it clearly stipulates the charging rules for secondary use: firstly, data processors and controllers may charge fees for the secondary use of health data. If the data is not held by the data acquisition institution or public sector, compensation for the specialized collection of health data must be paid, and the portion related to the data controller should be paid to the data controller; Secondly, any fees charged by data processors or controllers to data users should be transparent and in proportion to the cost of collecting and providing health data for secondary use. They should be objective, reasonable, and not restrict competition; Thirdly, when determining costs, the specific interests and needs of small and medium-sized enterprises, public institutions, institutions involved in researching health policies, and medical institutions should be taken into account, and these costs should be reduced proportionally based on their size or budget; Fourthly, if the data processor and data user fail to reach an agreement on the fee within one month after obtaining the data license, the health data access agency may determine the fee based on the cost ratio of providing health data for secondary use; If the data holder or user does not agree with the fees set by the health data access agency, they may resort to dispute resolution mechanisms.

In addition, the European Health Data Space Regulation also specifies other obligations for data processors and data users. Firstly, comply with data processing/usage principles. Including legality, reasonableness, transparency, purpose limitations, data minimization, accuracy, limited storage time, data integrity, confidentiality, and accountability. Secondly, comply with and assist patients in realizing their rights. This includes the right to be informed, access, correction, deletion, restriction of processing, data portability, opposition, and personal decision-making. Thirdly, the purpose of data processing must be legal, and the following four situations of data processing are considered legal:

obtaining the patient's explicit consent; handling health and medical data in emergency situations; processing health and medical data for specific medical professional purposes; processing for the public interest.

### 3.4 Data Regulator: Standardizing Institutional Arrangements and Organizational Systems

In terms of institutional arrangements, the European Health Data Space Regulation not only needs to fully comply with GDPR, but also needs to develop a "GDPR+" system that adapts to the free flow, effective control, and convenient access of health data,[7] including legal and regulatory frameworks such as the EU Medical Device Regulation, Data Governance Law, Data Law, Artificial Intelligence Law (Draft), and Regulation on the Protection of Natural Persons in the Processing of Personal Data by Trade Union Groups, Offices, and Institutions. In addition, GDPR regulatory safeguards are combined with other regulatory safeguards, including competition law, drug regulatory requirements, and EU AI regulations, to enhance the protection of health data regulatory mechanisms.

In terms of organizational structure, the European Health Data Space has established corresponding data regulatory agencies at both the member state and EU levels. For the one-time utilization of health data, each member state shall establish a digital health institution, whose responsibilities include: establishing relevant rules, developing MyHealth@EU, collaborating with member state authorities and stakeholders to address interoperability issues. For the secondary utilization of health data, each member state should establish a health data access agency, mainly responsible for collecting and compiling health data from different data holders to make it accessible, and handing over these data to data users for processing in a secure environment, jointly monitoring the quality and utility of the data with data holders. At the EU level, the European Health Data Space Committee is established, consisting of senior representatives from all member states' digital health authorities and health data access agencies. The European Data Protection Board and European Data Protection Supervisors can also participate, mainly responsible for assisting member states in coordinating matters between digital health agencies and health data access agencies, and promoting cooperation among relevant stakeholders. The EU Infrastructure Joint Control Group is responsible for handling the issue of joint control over cross-border infrastructure.

## 4 Challenges and Improvement Strategies of Personal Health Data Sharing in China

### 4.1 The Realistic Dilemma of Personal Health Data Sharing in China

At present, China's national health information platform has been set up, and provincial health information platforms are constantly improving. Over 8000 hospitals at or above level 2 are connected to the Regional Health Information Platform, and over 80% of tertiary hospitals in 20 provinces are connected to MHP.25 provinces have carried out electronic health record sharing and retrieval within the province, 17 provinces have carried out electronic medical record sharing and retrieval within the province, and 204 prefecture level cities have carried out interoperability and sharing of examination and testing results.[8]

While the health information platform is constantly improving, current health and medical data managers in China still face the dilemma of being afraid to share or unwilling to share. The main reasons for this are manifested in the following three aspects: firstly, the difficulty of ensuring the privacy and security of health data is high. Although China proposes to strengthen the standardization and security management of health and medical data, such as establishing strict electronic real name authentication and data access control. However, with the increasing popularity of wearable devices such as smart bracelets and smartwatches, people often encounter situations where personal health information is excessively collected, improperly utilized, or even leaked due to the "one package" consent authorization when accepting health management.[9] Secondly, there are relatively few legal regulations on health data, and it presents a fragmented phenomenon. At present, limited laws and regulations in China, such as the Cybersecurity Law, Personal Information Protection Law, Information Security Technology Personal Information Security Specification, and Key Information Infrastructure Security Protection Regulations, include medical and health information as key information within their regulatory scope. However, the Information Security Technology-Health and Medical Information Security Guidelines, Basic Medical and Health Promotion Law, and others have put forward relevant requirements for the use, disclosure, and informatization of personal health information. But this series of scattered and fragmented legislation cannot effectively regulate the flow of health data, and therefore cannot promote the reasonable sharing and use of health data. Thirdly, the collaboration mechanism between platform departments is not sound, and the technical standards are not unified. Although significant progress has been made in the development of information technology for national health in China, the construction of a business collaboration system for health data sharing is progressing smoothly. However, due to the vast territory of our country and the significant differences in economic development among different regions, economically underdeveloped areas have weaker ability to promote the development of health data informatization, inevitably resulting in significant differences in the degree of informatization of medical institutions at different levels and in different regions.

In addition, the scope of health data sharing is usually limited to institutions and platforms engaged in similar businesses, and there is a lack of communication and linkage with administrative departments such as disease prevention and control centers, medical security, and social security, making it difficult to organize collaboration and reach consensus among diverse data subjects. Only by achieving unified standards for health and medical data can the circulation and sharing of data be achieved without barriers. However, current health and medical data come from different information systems, including medical institution information management systems, clinical information

systems, image archiving and communication systems, radiology information management systems, electronic medical record systems, and computer-aided detection software systems. These systems have different hardware configurations, software settings, and information acquisition standards, making it difficult for data exchange and information sharing between different systems, resulting in a large number of “information islands”. In the process of data accumulation, there may be inconsistencies in the electronic and informational names of medical proprietary terms, such as multiple expressions of a disease, leading to problems in the integration between systems.

### 4.2 Strategies for Improving Personal Health Data Sharing in China

(1) Improving relevant legislation to fully safeguard the sharing of personal health data

Due to the lack of a clear definition of the ownership of health data in China's current legal system, there are many constraints in achieving consensus on open sharing of health data among different parties; At the same time, the legal norms that regulate the security of medical data are mainly principle norms, which are relatively general and vague in content, resulting in a lack of operability in practice and difficulty in guiding the medical industry to establish a data security protection system that is in line with its own characteristics.[10] Therefore, a balance should be struck between open sharing of health data and privacy protection, with reasonable and legal sharing as the premise and foundation. The objects, forms, and boundaries of health data sharing should be clarified as soon as possible, and the ownership relationship of health data and the rights and obligations of data subjects and data controllers should be clarified.

Based on the sensitivity and privacy protection requirements of health data, scientific classification and risk level classification should be carried out for this type of data. Protection standards, review rules, and even special legislation should be set from the perspectives of content security and technical security to establish a complete institutional system guarantee for health data sharing. In addition, it is also possible to consider establishing a digital identity management system for health data, including medical and health institutions and related personnel nationwide, and conducting electronic real name authentication to ensure that all operations of relevant personnel in the system are traceable, clarify the responsible parties, and play a warning and regulatory role. At the same time, a security review system should be established for data platforms and service providers, taking the security and reliability of the platform as risk assessment factors. Platforms or service providers with higher risk assessment levels should be warned and ordered to rectify. All the above measures should run through the entire process of data collection, use, disclosure, and even cross-border transmission, and implement full cycle and full scenario regulations on the sharing of health data.

(2) Protecting patient privacy to safeguard the exercise of data subject rights

Compared with the European Union, China's legislative protection of the right of data subjects to self-determination is relatively weak. The Personal Information Protection Law of our country provides relatively complete rights for personal information subjects, such as the right to know, access, correction, deletion, and portability. To consolidate patients' autonomy over data on this basis, the focus is on protecting their privacy rights. Firstly, it is necessary to improve the rules of informed consent. Currently, scholars have explored different forms of informed consent, such as generalized informed consent, consent with exclusion clauses, dynamic consent, and classified, stratified, and staged consent.[11] At the same time, the EU's "explicit consent" can also be used as a reference to adopt different forms according to the different categories of health and medical data, in order to achieve a balance between data utilization and privacy protection. Secondly, improve the mechanism for de labeling health data. The anonymization mechanism for health and medical data needs to be combined with other personal data protection measures, such as pseudonymization, to remove background knowledge and other relevant information from anonymized data as much as possible.

(3) Strengthening the construction of technical standards to promote trustworthy circulation among data controllers

One of the advantages of the European Health Data Space is the strengthening of consensus in the development and implementation of technical standards, setting common data identification, storage, sharing and utilization standards, and unified technical infrastructure for all parties to promote the trustworthy circulation of data. Drawing on the experience of the European Union, China can build cross regional health and medical data service infrastructure at the regional level, such as electronic health data cross regional sharing platforms, to promote data exchange and interoperability at the regional level, so that citizens and medical personnel can safely and efficiently access and utilize medical and health data. At the same time, attention should be paid to the construction of medical electronic record systems and corresponding interoperability standards should be established to improve the efficiency and transparency of data controllers in accessing and sharing data.

(4) Clear profit rules to safeguard the legitimate interests of data processors and users

Clarifying the obligations and profit distribution rules of data processors and users by learning from the European Health Data Space. On the one hand, relevant data processing institutions or organizations should take sufficient measures to ensure that processing activities in the field of health and medical data in accordance with legal and administrative provisions, and reasonably delineate the operational authority of health and medical data processing in accordance with the classification management norms of the "Health and Medical Data Security Guidelines", ensuring the confidentiality, integrity, and flexibility of data processing and use. On the other hand, it is necessary to improve the profit distribution mechanism between data processors and users. Sorting out the essential categories of health and medical data, considering the differences in the realization of the rights and interests of the roles carried by the data. If privacy and sensitive information are involved, it is advisable for the relevant data rights to belong to the original data provider or the government; If the data has been de identified, the attribution of rights can be confirmed based on

factors such as funding, technology, and labor (such as data production and processing), achieving the principle of "who inputs, who contributes, and who benefits", ensuring that all relevant parties can obtain reasonable benefits from their contributions, and reflecting the concept of balancing the promotion of data element utilization and the distribution of data benefits.

**FUNDING**

This work was supported by the Youth Fund for Humanities and Social Sciences Research of the PRC Ministry of Education [23YJC820006].

**COMPETING INTERESTS**

The authors have no relevant financial or non-financial interests to disclose.

**REFERENCES**

[1] National Information Security Standardization Technical Committee, Guidelines for Information Security Technology, Health and Medical Data Security [EB/OL]. 2020. http://www.phic.org.cn/zcyjybzpj/bzypj/bzgf/gjbz/202103/P020210331605989883649.pdf?hmpvqezfbjjzwskb.

[2] Victoria H. Data Protection Compliance in the Age of Digital Health. European Journal of Health Law, 2016, 23(3): 248-264.

[3] Wang Liming, Data Sharing and Personal Information Protection. Modern Law. Modern Law Science, 2019, 41(1): 45-57.

[4] Jingjin Sl, Rui Y, Xueming Y, et al.Factors Influencing the Sharing of Personal Health Data Based on the Integrated Theory of Privacy Calculus and Theory of Planned Behaviors Framework:Results of a Cross-Sectional Study of Chinese Patients in the Yangtze River Delta. Journal of medical Internet research, 2023, 25: e46562.

[5] Chen Yi, Research on Health and Medical Data Sharing and Personal Information Protection. Journal of Information, 2023, 42(5): 192-199.

[6] Baines R, Stevens S, Austin D, et al. Patient and Public Willingness to Share Personal Health Data for Third-Party or Secondary Uses: Systematic Review. Journal of medical Internet research, 2024, 26: e50421.

[7] Gerardo Fortuna. Commission wants GDPR+ protection to facilitate health data revolution[EB/OL]. 2024. https://www.euractiv.com/section/health-consumers/news/commission-wants-gdpr-protection-to-facilitate-health-data-revolution/.

[8] Jin Zhenya, The National Health Information Platform for All has been Basically Established. Guang Ming Daily, 2023.

[9] Wei Mingyue, Cui Wenbin, Wang Shu. Risk Analysis and Control Strategy of Internet Hospital. China Health Resources, 2020, 23(2): 99-101.

[10] Liu Junping, Huang Zeyu. The Dilemma of Medical Data Security and Its Solution Path. Medicine and Law, 2023, 15(5): 14-19.

[11] Jiang Hui, Yuan Minyi, Lian Ana. Pre-authorization System for Ethical Review and Informed Consent Implementation in Medical Institutions -Based on Research Involving Human Health Information and Biological Samples. Chinese Medical Ethics, 2021, 34(4): 414-421.