

Research on Internet Medical Data Security Issues under the Personal Information Protection Law

Jinyu Li

Kunming Medical University, Yunnan, China

1105886144@qq.com

Abstract. With the in-depth advancement of "Internet +", Internet medical treatment has achieved continuous development and innovation under the support of national policies. In the mode of Internet medical care, due to the vulnerability of the amount of medical data, the diversity of subjects involved and the commercial value, many problems of infringing on the medical data of patients have been caused, and the risk of improper leakage of medical data of patients has also been exposed. After the implementation of the "Personal Information Protection Law", it provides a legal protection barrier for Internet medical data, but the "Personal Information Protection Law" has the problem that the administrative protection field is not fully clarified and the protection of public and private laws needs to be further connected. Further strengthen the protection of Internet medical data under the Personal Information Protection Law by improving the coordination and coordination of public and private protection measures for medical data, clarifying the division of administrative supervision departments and responsibilities for Internet medical data, and formulating scientific and reasonable administrative discretion benchmarks.

Keywords: Internet medical treatment; medical data; personal information; protection mechanism

1. Overview of Internet Healthcare

1.1 Definition and development of Internet medical care

1.1.1. Definition of Internet Healthcare

Internet medical care is an innovative product formed by the continuous in-depth integration and development of Internet technology and medical level. Different from the traditional medical model, "Internet medical treatment" refers to a new medical model, that is, a medical practice driven by Internet technology. Interactive activities such as remote diagnosis and treatment, consultation, etc., cover many aspects such as marketing in Internet medical services, building doctor - patient relationship, providing medical advice, issuing prescriptions, and selling drugs and equipment. Medical institutions, on their own or in cooperation with third-party institutions, conduct diagnosis and treatment activities for patients through their online diagnosis and treatment platforms. At the same time, due to the lack of professional instruments and equipment for diagnosis on the online platform, it is difficult to draw a comprehensive diagnosis conclusion for intractable diseases. Internet diagnosis and treatment can only be carried out when the two conditions of "some common diseases and chronic diseases" and "revisiting" are met at the same time. In addition, Internet diagnosis and treatment also requires medical institutions to obtain a "Medical Institution Practice License" and requires physicians to have more than 3 years of independent clinical work experience. This move limits the basic framework of Internet medical care in terms of subject qualifications and the scope of diagnosis and treatment, and is intended to ensure the safety of people's health and the accuracy of diagnosis.

1.1.2. Development overview analysis

With the continuous and in-depth advancement of "Internet +", the State Council issued the "Guiding Opinions on Actively Promoting the "Internet +" Action" document in 2015 to support and encourage the active use of the Internet to provide services such as online diagnosis and treatment. Build a shared service platform for medical information services such as medical

imaging, electronic medical records, health files, and inspection reports that third-party institutions participate in . This document draws a grander blueprint for Internet medical care . In the following years, the number and scale of Internet hospitals have sprung up in China . In 2018, the National Health Commission and the Administration of Traditional Chinese Medicine jointly issued three documents related to the development of Internet hospitals , including the "Administrative Measures for Internet Diagnosis and Treatment" , which further serve as the industry code of conduct for Internet hospitals, defining the outline for the development of Internet hospitals and clarifying the development pattern. , according to the data survey of Zhongguancun Industrial Research Institute , in 2019, the number of Internet hospitals with physical hospitals as the main body increased sharply, from 21 in 2018 to 173, with a growth rate of 723.8%. After 2020, continue to maintain the growth trend. [2] Under the background of the new crown epidemic , the people's demand for Internet diagnosis and treatment has increased significantly . In May 2020, the National Health and Health Commission issued the "Notice on Further Improving the Appointment and Treatment System and Strengthening the Construction of Smart Hospitals" . With the clear and specific requirements for the construction of Internet hospitals, the construction of modern information hospitals with electronic medical records as the core has become a newer construction direction . However , with the in - depth development of Internet hospitals , while Internet hospitals have brought convenience , many risks related to patient medical data leakage have also been exposed . The form responds to the issue of personal information data protection related to the interests of every citizen , and responds to the problem of " legislation decentralization" of personal information protection that has been called for by academic circles in the past . The trend and trend of chemical protection conforms to the development of Internet hospitals, and at the same time protects the data health and privacy security of patients from the legal level .

1.2 Characteristics of medical data

1.2.1.Vulnerability of medical data

The development of big data is changing rapidly , and medical data is also increasing with the continuous increase of the number of patients and the rapid development of Internet hospitals. The comprehensive and specific records of patients' information including heart rate , blood sugar , weight , electrocardiogram , blood pressure and other information also lead to the multiplication of medical information. , medical data is most typical of gene sequence data . According to research , it is estimated that 2 billion sets of human gene sequences will be formed by 2025, and the storage requirements of these data alone may be as high as 40 exabytes, while the total storage capacity of the entire Internet is estimated to be no more than 525 exabytes. The huge number and scale of medical data have ushered in a huge challenge for patient data protection . Huge medical data requires a huge system to adapt to the progress and innovation of medical care. And the increase in the difficulty of protection in the process of protection . What's more , data in electronic form is often more vulnerable to intrusion , access , copying and theft by illegal technical means than traditional paper version of patient medical information . The huge scale of medical data makes it difficult to protect medical data in an all-round way , and medical data stored in electronic form is vulnerable to improper processing on the Internet platform . Therefore , medical data is more vulnerable than general data .

1.2.2.The value of medical data

Because medical data contains the real personal information of patients , there are many private information related to their own interests that patients are unwilling to actively disclose and disclose . These data information is an identifier of personal identity . Commercial interests are often contained in these data closely related to individuals . For example, pharmaceutical companies will develop and sell medicines related to patients based on the medical and health data of patients ; After systematic analysis , it provides patients with health management services and displays

different products ; Unlawful data processors, driven by their interests, steal and sell the collected patient data without the permission of the patients themselves ; there are still a large number of criminals who pass Illegal technical means to obtain patient medical information for profit . It can be seen that the sensitivity of medical data itself shows a lot of commercial value under the analysis and operation of big data . At this time , it is necessary to comprehensively strengthen the protection of patient data to ensure the realization of patients' right to decide and delete personal information. .

1.2.3.The diversity of subjects involved in medical data

In the operation of Internet medical care, there are many subjects involved: the most basic is the relationship between the diagnosis and treatment between the hospital and the patient , and the relationship between the patient and the medical service . For the third-party data processor that provides a medical treatment platform , this is also a new subject compared to the traditional medical model , that is, one of the data processors of medical data . Again , it also includes technical personnel who integrate and organize the data . At the same time, it includes the Health and Health Commission, which conducts external administrative supervision of Internet hospitals and conventional hospitals, and other administrative departments coordinated by the national network information department that supervises data security as stipulated in the Personal Information Protection Law . In the process of diagnosis and treatment, multiple parties have more or less contact , management , and use of patients' medical data. In any part of the operation of medical data, there will be risks and possibilities of data leakage and theft . Therefore , the diversity of subjects in Internet medical care has brought new challenges to the security protection of patient data , and there are also difficulties in distinguishing and tracing the responsibility for data leakage .

1.3 Legal review of privacy and data protection of Internet medical patients

From the perspective of legislation, the law attaches great importance to the protection of medical data in my country at present. Regarding the protection of patients' personal information, the law first appeared in Articles 55 and 56 of the Tort Liability Law, and was later absorbed and integrated in the Tort Liability Section of the Civil Code. Article 1225 of the "Civil Code" stipulates that medical institutions and internal physicians and staff shall record and save patients' hospitalization records, examination reports, records of doctors' orders, medical care information, and information on surgery and anesthesia in strict accordance with regulations. , When copying the relevant case data, the medical institution has the responsibility and obligation to provide it. Article 1226 of the "Civil Code" stipulates that medical institutions and their doctors and other medical workers are responsible for keeping the personal information of patients and the privacy part that they do not want to disclose. responsibilities of rights. In the field of health law, Article 22 of the Law on Licensed Physicians stipulates that physicians shall fully respect and protect the privacy of patients when conducting diagnosis and treatment activities within the scope of their duties, and dutifully protect the privacy and security of patients. Article 12 of the Law on the Prevention and Control of Infectious Diseases stipulates that disease prevention and control institutions and medical institutions need to protect the personal privacy and related personal information of patients, and shall not disclose or improperly disclose it. Article 34 of the "Law on Maternal and Infant Health Care" stipulates that the practice of maternal and infant health care has the duty of confidentiality for the parties concerned, and the practice principles and professional ethics must be adhered to. Afterwards, with the increasing attention of personal information protection in Jiangsu, Zhejiang, and Zhejiang, the implementation of Articles 40-50 of the Cybersecurity Law in 2021 requires network service providers to adhere to the principle of security and confidentiality when processing personal data, and not to illegally provide personal information. The Personal Information Protection Law, which is based on the protection of personal information, puts forward behavioral requirements and obligations for "personal information processors" as a whole, and systematically protects citizens' personal information and data privacy through legislation. A bold stroke.

2. Current Situation of Internet Medical Data Protection under the Personal Information Protection Law

2.1 Main body norm protection in Internet medical care

In the previous part of this article, the multi-party subjects involved in Internet medical care have been analyzed. It can be seen that the participating subjects under the mode of Internet medical care are diversified. Combined with the content of the "Personal Information Protection Law", in addition to the personal information subject who enjoys the relevant information protection rights, it is also proposed that the obligor subject to which the rights are directed is the personal information processor. This subject is the "Personal Information Protection Law". The most core subject, there are 41 articles about the behavior regulation and specific obligations of personal information processors in the laws and regulations, accounting for 1/2 of the number of articles. This legislation draws on the European Union's GDPR, Japan's Personal Information Protection Law and the US Federal Consumer Data Privacy and Security Act on the basis of comparative law. Protect. In the field of Internet medical care, in terms of the protection of data and rights of patients by medical data processors, it can also be seen from the analysis of the legal responsibility of China's Personal Information Protection Law below that it has risen to a higher level of responsibility. As the responsible subject, the processor of medical data needs to abide by stricter data protection rules and fulfill the responsibility of the first responsible person for data protection.

2.2 Analysis of the content of Internet medical patients' rights

In the process of Internet medical data protection, respecting the rights of patients to process personal information is the premise of realizing the rights and interests of personal information. As a representative of the civil law system in Germany, German scholars proposed the "right to self-determination of personal information" in 1976. Based on this right, the right holder should enjoy the rights of informed consent to personal information, and other rights are derived from the right to self-determination of personal information. . [3] The fourth part of China's "Personal Information Protection Law" specifically builds a rights system for the protection of personal information subjects in information processing activities, and the rights of personal information and the scope of protection have also been expanded. Among them, Article 44 establishes the right to know and the right to make decisions, which are the core of personal information rights. The right to know Under the operation of Internet medical care, patients are guaranteed to have the right to know their own relevant medical records, the processor of their personal data, the purpose and method of processing the data, and the specific content of the data processing; the right to make decisions is to protect the personal medical data of patients. In the process of processing, it is in a key and core position, and it has the right to independently decide the processing method and purpose of personal medical data, as well as the extent to which it is processed and used.

Articles 45, 46, and 47 of the Personal Information Protection Law establish, on the basis of Article 44, the rights of information subjects to copy and access, portability, supplementary correction and deletion. Through the exercise of this right, the personal information subject can clarify whether the data held by the personal information controller complies with the informed consent rules in the collection of personal information, and can measure whether the personal information protection principles such as data minimization and specific purpose have been complied with. Patients can exercise the right of copying and viewing to the medical data processor to consult and copy their case data, and the data processor should also provide it in a timely manner, but in the case of relevant public interests, this right needs to be given way to

protect public interests. Through the right of portability, patients can agree to decide the transfer of their medical data between different Internet platforms. If the patient sees a doctor on the Internet platform of the hospital, if a referral service is required, after obtaining the patient's permission, the original medical data processor can The format that conforms to the standard is passed to the third-party hospital Internet medical treatment platform to continue to complete the follow-up diagnosis and treatment activities. Patients can still exercise the right of supplementary correction and deletion to ensure the integrity of personal information and the integration of personal digital personality. This right enables patients to be the masters of their own information control, to deal with irrelevant and unnecessary relevant data related to diagnosis and treatment activities, and to make self-determination and choice of relevant private data that they do not want to disclose publicly.

The cooperation of the above rights is centered on personal control, and the personal information subject is given full control over personal medical data in the form of a bundle of rights. Under the operation of Internet medical care, fully guaranteeing and realizing the above-mentioned rights of patients to process personal information will help to coordinate the protection of personal information rights and the rational use of personal information.

2.3 Regulatory means for the protection of Internet medical rights

In order to fully guarantee the realization of information protection rights, respect the value of rights, and regulate personal data processors with strict responsibilities and obligations is crucial. Part V of the Personal Information Protection Act specifically provides comprehensive provisions for the obligations of data processors. In terms of data processor obligations, medical data processors need to fulfill their obligations to take corresponding encryption, de-identification and other security technical measures and classified management of patients' medical data to ensure the compliance of processing activities. According to the "Personal Information Protection Law" Articles 52-58 stipulate the personal information protection system, establish an impact assessment system for the protection of sensitive personal information, and information processors regularly undergo compliance audits and take remedial emergency measures in a timely manner. Among them, the requirements of medical data processors in Internet medical care are that they need to designate a protector who is responsible for supervising their actions and should submit the personal information of the protector to the relevant responsible department. This system establishes the data processor's The risk self-regulation and management model requires data processors to be sensitive to the risks of patient information protection at all times in a dynamic form, and to take measures in the most proportionate way to the purpose.

Since medical data falls within the scope of sensitive information referred to by this law, medical data processors in Internet medical care shall, before processing patient information, make in advance the purpose of processing, processing methods , security risks , and protection measures including personal information in accordance with legal requirements. Legal and appropriate personal information protection impact assessment report. Finally, in view of the huge amount of medical data and the characteristics of being easily infringed, medical institutions or Internet diagnosis and treatment platforms should also establish a personal information protection compliance system and regularly publish personal information protection social responsibility reports, accept social supervision, in order to better fulfill the "Personal Information Protection" compliance system. Obligations for personal data processors under Article 61 of the Data Protection Act.

2.4 Restriction of legal responsibility

The Personal Information Protection Law stipulates stricter legal responsibilities for personal data processors, and regulates the behavior of personal data processors with stricter legal responsibilities. Preventing the occurrence of illegal acts can be achieved by increasing illegal costs, so that offenders can promote the consideration of illegal costs before committing illegal acts, so as to reduce the occurrence of illegal acts. Part VII of the Personal Information Protection Law specifically stipulates data. The six articles stipulate more severe legal consequences, ranging from the civil liability of the handler for breach of duty to the administrative liability and even the corresponding liability of the criminal liability. The property penalty part can impose a fine of up to 50 million yuan on medical data processing institutions that seriously violate their obligations and impose a fine of up to 1 million yuan on the relevant responsible persons; the behavioral penalty part is in addition to violating the "Criminal Law". In addition, a new form of administrative punishment has been added, that is, applications that illegally process personal information are ordered to suspend or terminate the provision of services. This is a new type of administrative responsibility for governance, reflecting different characteristics from traditional administrative responsibility. Breaking through the traditional principle of responsibility, it has severe or aggravated punishment. It can be seen that the Personal Information Protection Law is an unprecedented breakthrough in the protection of personal information, and the non-palliative treatment of information leakers who violate their obligations has also laid a certain foundation for the development of Internet medical care.

3. Problems existing in Internet medical data protection under the Personal Information Protection Law

3.1 The remedies in public and private law still need to be further connected

Although there is a dispute between "public rights" and "private rights" in the protection of personal information rights and interests in the construction of China's personal information protection system, there are two views of civil remedies and administrative remedies for the remedy of personal information rights. However, China's personal information protection adopts dual rights protection and relief measures of public law and private law. Part VI of the "Personal Information Protection Law" specifically stipulates the administrative supervision and protection of personal information protection. Article 60 clarifies that the organization of personal information protection work and related supervision and management work shall be the national network information department to coordinate and coordinate other organs. Departments; Articles 61 and 63, in addition to requiring administrative supervision departments to perform their duties to protect personal information, also provide the administrative supervision departments may take measures to inquire, investigate, consult, copy relevant materials, conduct on-site inspections, and investigate violations of personal information processing agencies. Administrative law enforcement measures such as seizure and seizure of items; at the same time, Article 64 stipulates that for major security incidents involving personal information, the relevant administrative departments may interview the information processor and the responsible person, and may also entrust a specialized information protection compliance agency to process personal information and data. Institutions conduct compliance reviews and criminal responsibility for linked personal information crimes. For the protection of personal data, the above administrative supervision measures have the advantages of professional information as a public power, the efficiency of preventing and dealing with systematic violations, and the advantages of forming general rules, but they also consume more public resources and cannot provide victims with materials. Compensation and other disadvantages.

Compared with the protection methods of public power, the Civil Code and the Personal Information Protection Law jointly provide civil remedies for persons whose personal information

rights and interests have been infringed: on the basis of the principle of presumption of fault, the victim may In addition to self-relief for personal information processors, the civil public interest litigation stipulated in the Personal Information Protection Law can be used as a supplementary remedy to protect self-rights. Compared with administrative remedies, civil remedies have the advantages of more flexibility and lower litigation costs, but at the same time, due to the large difference in the professional and technical levels of personal information processors and victims, the former has an absolute advantage , which makes it difficult to safeguard rights . problems and the long period of judicial decisions to respond to cases, which leads to the delay in the overall governance level of the society.

Administrative protection and civil protection have their own advantages and disadvantages in their respective fields. They should not be mutually exclusive, but should be coordinated and coordinated with each other. The protection of personal information rights cannot rely on a single public and private field to achieve the function of comprehensive relief. The intervention and assistance of public power can help improve the situation where the data victim is at an absolute disadvantage in the professional and technical fields. The flexibility of private rights is also realized. An effective path for the specific interests of the parties. Both relying too much on a certain method cannot better achieve the legislative purpose and purpose of the "Personal Information Protection Law". In the process of practical application of the "Personal Information Protection Law", the connection and supporting mechanism between the two still need to be further improved. A protection model in which civil is connected with administration, and administrative is connected with criminal. On the basis of mutual coordination and complementation of advantages and disadvantages, the three are a relatively considerable protection system for personal information rights and interests.

3.2 The administrative subjects of medical data supervision are scattered and the division of responsibilities is unclear

The "Personal Information Protection Law" stipulates that the administrative supervision agency for personal information protection is the national cybersecurity and informatization department and other departments under its overall coordination. At the same time, "relevant laws and administrative regulations" also have room for the division of supervisory responsibilities. In this regard, the provisions of "other departments" are relatively broad and unclear. Many departments, including the public security department, the national network information department, and the industry and information department, all have responsibilities and obligations for data supervision. There is still a lot of room for regulation and room for the division of powers of various departments. In the field of Internet medical care, such a relatively decentralized regulation. In the process of administrative supervision of Internet medical care, there is a lack of clear division of responsibilities and overall planning among multiple departments with law enforcement power, which will lead to a regulatory vacuum in the protection of personal medical data. It is not conducive to the unified supervision of the national network information department, nor is it conducive to creating a unified and centralized administrative protection environment for the development of Internet medical care. Due to the ambiguous division of powers between different departments, the problems of work efficiency and law enforcement capabilities are also not conducive to the healthy development of Internet medical care.

In addition, there is another dilemma: the protection of personal information in the medical field is different from that in other fields. As a comprehensive regulatory agency, it is difficult for the national network information department to fully understand the characteristics of the medical industry. Data in different fields have different characteristics. Personal information data in the financial field, medical field, etc. has a strong professional nature. The supervision scheme formed by the direct management of comprehensive institutions is often difficult to prescribe the right

medicine, and it is difficult to treat patients in the Internet medical field. Personal medical data forms effective data compliance supervision.

3.3 The scope of punishment is too broad and lacks a benchmark for discretion

In order to regulate the behavior of personal information processors with strict legal responsibilities, Article 66 of China's "Personal Information Protection Law" imposes a fine of less than one million yuan on personal information processing institutions that violate their obligations, and the person directly responsible can be fined less than one million yuan. A fine of 10,000 yuan to 100,000 yuan is imposed; for serious circumstances, a fine of not more than 50 million yuan can be imposed on relevant institutions, and a fine of not less than 100,000 yuan but not more than 1 million yuan can be imposed on those directly responsible. It can be seen that the amount of administrative penalty in this regulation has a very wide discretionary space. As a normative document in China, the administrative discretion benchmarks clarify the scope of punishment in a specific and clear way. The specific discretionary behaviors made are controlled within a reasonable range and standards, improve the visualization of the discretionary operation process, cultivate normative value identities, promote the individual's value belief in discretion, and shape the individual into the subject of normative awareness. This is also a good means for administrative organs to improve their own law enforcement capabilities, self-supervision and restraint, control self-administrative powers, and improve the rationality and fairness of law enforcement.

However, since the Personal Information Protection Law will not be implemented until the end of 2021, the supporting measures of legislation often have a certain lag. Therefore, the current regulations on the discretionary benchmarks for the corresponding administrative penalties for Internet medical data processors who violate the prescribed obligations are still in a state of absence. The problem brought about by the lack of specific discretionary benchmarks is: although the administrative penalties made by the administrative organs are within the legal range, the specific penalty amount made will not be reasonably changed due to different circumstances and other relevant factors. Just reasons to explain the rationality of punishment will lead to the abuse of public power, and will also bring excessive and unnecessary burdens to medical data processors, which is not conducive to the standardization and rationality of Internet medical treatment in terms of administrative protection.

4. The Perfect Path of the Personal Information Protection Law in Internet Medical Protection

4.1 Improve the connection between public and private laws in the protection of personal information

China's personal information protection law not only reflects the norms of private law but also has the content of public law, the two have achieved an organic integration to a certain extent, and systematically is an integrated protection model of public and private law. As explained above, administrative relief and civil relief have their own unique advantages and disadvantages, and they will play different functions and roles in different situations. The reason for the highly integrated protection of public and private laws in the special field of "personal information protection" is that unequal relationships have political connotations and governance needs, and a purely unequal relationship cannot draw the conclusion that the law is inclined to protect. Internet medical data also belongs to a special field, and the unequal status between information processors and patients needs legal protection. The "Personal Information Protection Law" protects it as "sensitive information" and builds a coherent framework for public and private law protection measures. In this regard, it is necessary to establish a systematic protection model in which public and private laws are further coordinated and connected.

The connection between public and private laws of personal information protection can be reflected in the layered protection of sensitive personal information . The sensitive information is combined with other relevant factors and variable factors to comprehensively consider the protection level division . On the basis of the classification of personal information in the field of public and private law , different Levels of protection for choosing different measures to protect . It can provide different levels of protection for administrative organs for different levels of data . It can not only coordinate administrative law enforcement resources , but also concentrate law enforcement forces to give more supervision and protection to data with high intensity in sensitive medical data, and further improve Convergence protection of public and private laws in personal information protection . In addition to the exception , the connection between public and private law protection of personal information protection must be coordinated with other laws such as civil law , criminal law , administrative law , cybersecurity law, etc. , so as to realize the rational connection and integrated protection of personal information protection between public and private laws, and fully from the legal level . Build barriers to the protection of personal information rights .

4.2 Clarify the division of medical data supervision subjects and responsibilities

In view of the current situation that China's data protection supervision subjects are scattered and the responsibilities of different departments are unclear . The urgent problem to be solved now is to clarify the "other departments" in the " Personal Data Protection Law " that are coordinated by the national public information department . In view of medical data as sensitive data and its characteristics, combined with the specific national conditions of our country , the data supervision subjects in the Internet medical field should be specifically refined , and it should be clarified that professional institutions should conduct medical data processors under the overall coordination of the national network information department. special regulation .

Secondly , it is necessary to specifically divide the responsibilities of the multiple departments responsible for data supervision and the specialized medical data supervision agencies mentioned above , and clarify the priority of responsibilities between different departments , so as to avoid the problem of mutual shirk. The medical field includes the important role played by specialized medical data regulators in the Internet medical field . Improve the management and supervision system for the behavior of medical data supervisors within the professional medical data supervision department , protect medical data at different levels to different degrees , and carry out key supervision of key medical data . Due to the strong liquidity of data , it is difficult to measure and calculate the flow range of data , and it is difficult to specifically assess the risk of data dissemination . Therefore , it is reasonable and necessary to change the post-supervision status of traditional administrative agencies and conduct pre-supervision and precautionary measures for the behavior of medical data processors .

4.3 Establishing a reasonable benchmark for punishment and discretion

Due to the lack of a unified discretionary benchmark for administrative penalties , medical data supervisory authorities in different regions will impose different penalties for similar behaviors made by medical data processing institutions that violate their obligations in the application of the Personal Information Protection Law . The result of this punishment is not conducive to establishing the authority and impartiality of the administrative organ . Regarding the broad scope of administrative penalties and the unclear expression of " serious circumstances" in the Personal Information Protection Law , a clear and further explanation should be made , and scientific and reasonable benchmarks should be set .

To formulate scientific discretionary benchmarks, we must first accurately grasp the relationship between "rationality" and "legality". In terms of legality, it not only requires the punishment of medical data processors who violate their obligations to be within the scope of punishment stipulated by law, and divides the scope into different levels according to the circumstances of the case, but also demonstrates the purpose and purpose of legislation; in terms of rationality, It is

required that the current situation of various regions in China due to differences in economic development and imbalances between regions should be considered under the premise of comprehensively considering the facts of improper processing of medical data , the current situation of social Internet medical development , hospital cultural background , serious circumstances , social impact and other related factors . Each region needs to formulate a unified discretionary benchmark within its region to adapt to the actual local development. Finally , the relevant factors considered in the formulation of discretionary benchmarks are abstract to a certain extent . In the face of complex social changes and unpredictable social realities , it is not comprehensive to rely only on discretionary benchmarks to cover all possible realities . It is necessary to give full play to the regulatory awareness of the medical data supervisory authority to formulate corresponding discretionary benchmarks . Only in this way can it achieve complementary advantages between restriction and freedom, and achieve a good law enforcement effect .

5. In conclusion

Based on the current situation , personal information protection has become the consensus of the whole society . The legal community is also responding to the concerns of all walks of life and formulating relevant departmental laws to protect personal information and data security . The patient medical data involved in Internet medical care is exactly a type of data that is clearly classified as sensitive personal information in the Personal Information Protection Law , which requires special attention and protection in the process of implementing this law . Although a system for protecting personal information has been established between different laws , especially the Personal Information Protection Law , which systematically protects personal information , there are still areas in its specific content that require further coordination and improvement of public and private laws . With the focus on the field of Internet medical care, more specific and professional administrative supervision agencies are required to provide detailed and clear administrative supervision of medical data . At present , Internet medical care is booming . With the further improvement and protection of patients' medical data security by laws and relevant administrative regulations and policies, the rights and interests of patients' personal information will fully realize their legal value .

References

- [1] Reed J. Cybermedicine:Defying and Redefining Patient Standards of Care[J]. Indiana Law Rev, 2004, 37 (03):845-877.
- [2] Data source : <https://www.cn-healthcare.com/articlewm/20210603/content-1227578.html>
- [3] Gao Fuping. Personal Information Protection: From Personal Control to Social Control [J]. Legal Research, 2018, 40(03): 84-101.
- [4] Li Weiqun, Guo Yu. Research on the Legal Issues of the Commercial Application of Health and Medical Data [J]. Qilu Journal, 2021(04):96-103.
- [5] Article 1225 of the Civil Code
- [6] Article 1226 of the Civil Code
- [7] Article 22 of the Law on Practising Physicians
- [8] Article 12 of the Law on the Prevention and Treatment of Infectious Diseases
- [9] Articles 40-50 of the Cybersecurity Protection Law
- [10] Hu Wentao. Conception of the definition of personal sensitive information in China [J]. China Law, 2018(05):235-254.DOI:10.14111/j.cnki.zgfx.2018.05.013.
- [11] Wang Liming, Ding Xiaodong. On the Highlights, Features and Application of the Personal Information Protection Law [J]. Jurist, 2021(06):1-16+191.DOI:10.16094/j.cnki.1005-0221.2021.06.001 .
- [12] Wu Weiguang. Criticism of personal data privacy protection under big data technology [J]. Politics and Law, 2016(07):116-132.DOI:10.15984/j.cnki.1005-9512.2016.07.011.

- [13] Jiang Ge. Choice of Legislative Model of Personal Information Protection Law — — From the Perspective of German Experience cnki.1674-5205.2011.02.003.
- [14] Wang Qinghua. A Systematic Interpretation of the Right to Personal Information——Also on the Public Law Attribute of the Personal Information Protection Law [J]. Global Law Review, 2022, 44(01): 69-83.
- [15] Wang Liming, Ding Xiaodong. On the Highlights, Features and Application of the Personal Information Protection Law [J]. Jurist, 2021(06):1-16+191.DOI:10.16094/j.cnki.1005-0221.2021.06.001 .
- [16] Long Weiqu. The Basic Law Positioning and Protection Functions of the Personal Information Protection Law: An Analysis Based on the Formation and Development of the New Legal System [J]. Modern Law, 2021, 43(05): 84-104.
- [17] Wang Xixin, Peng Kun. The Constitutional Basis of the Personal Information Protection Legal System [J]. Tsinghua Law, 2021, 15(03): 6-24.
- [18] Kong Xiangwen. On the Administrative Regulation Path of Personal Information Protection [J]. Administrative Law Research, 2022(01):131-145.
- [19] Cheng Xiao. Innovation and development of China's "Civil Code" personal information protection system [J]. Finance and Economics Law, 2020(04):32-53.DOI:10.16823/j.cnki.10-1281/d.2020.04. 003.
- [20] Liu Xiaochun. The industry standard-led model of personal information protection in the era of big data [J]. Finance and Economics Law, 2017(02):11-21.DOI:10.16823/j.cnki.10-1281/d.2017.02.002.
- [21] Kong Xiangwen. On the Administrative Regulation Path of Personal Information Protection [J]. Administrative Law Research, 2022(01):131-145.
- [22] Peng Kun. On the Administrative Penalty System for Personal Information Protection——Centered on Article 66 of the "Personal Information Protection Law"[J/OL]. Administrative Law Research, 2022(04):1-12[2022-05-18].<http://kns.cnki.net/kcms/detail/11.3110.d.20220511.1550.003.html>
- [23] Xia Qingfeng. Improvement of notification obligations and dynamic anonymization of personal information protection in cyberspace [J]. Jiangnan Forum, 2022(03):95-103.
- [24] Bao Lufan. Institutional Positioning of Discretionary Benchmarks: Standardization of Reasons
- [25] Wang Chuanqian. Research on the technical paradigm of administrative discretion benchmarks [J]. North Law , 2013,7(03):154-160.DOI:10.13893/j.cnki.bffx.2013.03.007.
- [26] Ding Xiaodong. How does the law adjust the unequal relationship? On the legal basis and institutional framework of the inclined protection law [J]. Chinese and Foreign Law, 2022,34(02):445-464.
- [27] Zhang Yong. Integrated Protection of Sensitive Personal Information by Public and Private Law
- [28] Huang Xuexian. Discussion on Several Issues of Perfecting Administrative Discretion Benchmarks [J]. Jianghai Journal, 2009, (6): 146.
- [29] Xiong Wenzhao. On the refinement of the discretionary benchmark for urban management law enforcement [J]. Administrative Management Reform, 2018(06):27-33.DOI:10.14150/j.cnki.1674-7453.2018.06.005.