

Research on Patient Privacy Protection Issues and Countermeasures in Medical Management

Xiran Feng

The First Clinical Medical College of Kunming Medical University, Kunming, Yunnan, 650500

ABSTRACT

With the acceleration of information technology, the importance of patient privacy protection in medical management is becoming increasingly prominent. The electronicization and information sharing of medical data have facilitated medical services, but also brought risks of privacy breaches. This article analyzes the current situation of patient privacy protection in medical management, explores issues such as incomplete laws and regulations, information technology loopholes, lack of awareness among medical staff, and deficiencies in hospital management systems, and reveals the main risk factors for patient privacy leakage. In response to these issues, this article proposes countermeasures and suggestions such as improving laws and regulations, strengthening information technology security, enhancing the awareness of privacy protection among medical staff, and improving hospital management systems to improve the level of patient privacy protection and ensure the healthy development of the medical industry.

KEYWORDS

Patient privacy protection; Medical management; Information security; laws and regulations; Technical countermeasures

1 Introduction

With the rapid development of information technology, the issue of patient privacy protection in medical management has gradually become a focus of social attention. The electronicization, information sharing, and cross institutional communication of medical data have facilitated medical services, but also brought the risk of patient privacy leakage. The existing privacy protection mechanisms still have many shortcomings in terms of law, technology, and management, which urgently need to be further explored and resolved. This article aims to analyze the issues of patient privacy protection in current medical management, explore the challenges it faces, and propose practical measures to provide theoretical support and practical guidance for ensuring patient privacy and safety and promoting the healthy development of the medical industry.

2 Analysis of the Current Situation of Patient Privacy Protection in Medical Management

2.1 Current Status of Privacy Protection in Medical Management

With the rapid development of medical informatization, the importance of patient privacy protection in medical management has gradually been emphasized. Currently, more and more medical institutions have realized that protecting patient privacy is an important aspect of improving medical quality and enhancing patient trust. Many hospitals have invested a lot of funds and technology in information management, establishing information platforms such as electronic health records and remote medical systems, and taking measures such as data encryption and identity authentication to protect patients' privacy. However, there are still certain differences in the current situation of privacy protection in medical management, especially in some small and medium-sized medical institutions and grassroots medical units, where the implementation of privacy protection measures is relatively weak, the level of information construction is low, and the support of technology and law is not yet perfect. Although some hospitals have implemented privacy protection policies and the management of medical information is gradually becoming standardized, overall, the mechanism for privacy protection has not yet formed a unified and perfect standard, and there are still many challenges to face.

2.2 Main Problems Existing

Although more and more hospitals have made efforts in privacy protection, there are still various issues regarding patient privacy protection in current medical management. Firstly, the laws and regulations are not yet perfect, and the existing privacy protection laws mainly focus on data protection and information security, lacking specific provisions for the medical industry, resulting in insufficient enforcement of patient privacy protection. Secondly, there are loopholes in the privacy protection management system within the hospital, especially in the process of information sharing and data transmission, where the hospital lacks effective monitoring and management, leading to an increased risk of information

leakage. Again, the awareness of privacy protection among medical staff is generally low, and some medical staff fail to strictly comply with privacy protection regulations, even intentionally or unintentionally disclosing sensitive information of patients. In addition, there are also security risks in information technology. The hospital's information system has vulnerabilities and fails to update system security patches or encrypt data in a timely manner, making patient information easily stolen by external attackers.

2.3 Risk factors for patient privacy leakage

The risk factors for patient privacy leakage mainly come from multiple aspects. Firstly, vulnerabilities in information technology are an important risk factor. With the popularization of information systems, the information management systems of many hospitals have gradually become weak links for privacy leakage. Many hospitals lack necessary encryption protection for their electronic health records and medical data, and have insufficient network security measures, making them vulnerable to hacker attacks or information tampering. Secondly, loose internal management in hospitals is also an important reason for privacy breaches. Some hospitals fail to strictly enforce patient privacy protection regulations and have lax management of information access permissions, resulting in employees or outsourced personnel potentially having unauthorized access to patient privacy information. In addition, insufficient awareness of privacy protection among medical personnel is also one of the risks. Some medical personnel fail to strictly maintain confidentiality, especially in the process of transmitting and sharing patient information, and fail to ensure that information is only used between authorized personnel. Finally, insufficient legal supervision is also one of the risk factors for privacy breaches. Existing laws and regulations have relatively light punishment for privacy breaches and lack effective constraint mechanisms. Hospitals' enforcement of privacy protection is insufficient, leading to frequent incidents of privacy breaches.

3 Challenges faced by patient privacy protection in medical management

3.1 Imperfectness and insufficient enforcement of laws and regulations

In medical management, the legal framework for patient privacy protection is not yet perfect, and existing laws and regulations have not fully covered all privacy protection needs, with weak enforcement. Although China currently has relevant laws such as the Personal Information Protection Law and the Cybersecurity Law, these laws focus more on network information security and personal information protection, and have not made specific details on privacy protection in the medical field. Especially in terms of cross institutional transmission and sharing of medical data, the lack of clear regulations and supervision can easily lead to the leakage of patient privacy information. In addition, the enforcement of patient privacy protection in judicial practice is insufficient, and many hospitals lack mandatory measures to address patient privacy protection, resulting in frequent cases of privacy breaches. The government and regulatory departments are still insufficient in strengthening the construction of laws and regulations, with ineffective implementation and enforcement of laws, and a lack of effective punishment mechanisms. The lack of timely and effective punishment from relevant departments for the hospital's oversight in privacy protection has resulted in a lack of legal binding force.

3.2 Vulnerabilities and Security Hazards in Information Technology

With the popularization of electronic health records and digital medical services, information technology has become an important component of medical management. However, technical vulnerabilities and security risks have become important sources of risk for patient privacy breaches. Currently, many hospital information systems have not taken sufficient encryption and protection measures, which poses a potential risk of data leakage. Especially in the process of information exchange and remote healthcare, due to the lack of comprehensive network security technology, patients' personal information is easily attacked or stolen by hackers. At the same time, some hospitals have loopholes in information system management, such as some hospitals not updating security patches in a timely manner, not conducting regular data backup and recovery drills, etc., which may result in ineffective protection of patient privacy information in the event of system attacks. Despite the rapid development of technology, the healthcare industry generally lacks investment in information technology security protection, especially in some small and medium-sized medical institutions where information technology security is still relatively weak.

3.3 Lack of Privacy Protection Awareness among Medical Personnel

Medical personnel are important executors of patient privacy protection, but currently many medical personnel still

have weak awareness of privacy protection and lack systematic training. Some medical personnel fail to fully understand and respect patients' privacy rights in their work, and even engage in the behavior of arbitrarily leaking patient information. The emergence of this phenomenon is closely related to inadequate privacy protection training and lack of awareness among medical personnel. Many hospitals' training on privacy protection for medical staff mainly focuses on onboarding, lacking regular retraining and updates. The legal and technical background of privacy protection is constantly changing, and medical staff often do not know how to respond to specific situations without continuous learning and practice. Some medical staff may share patients' personal information without their explicit consent due to work convenience or a sense of urgency for privacy protection, increasing the risk of patient privacy leakage.

3.4 Inadequate internal management system of the hospital

The privacy protection management system within hospitals is the core of ensuring patient information security, but currently many hospitals have problems with inadequate systems and poor execution in privacy protection management. Some hospitals have failed to develop detailed patient privacy protection policies and operating procedures, resulting in a lack of unified standards and guiding principles for employees in the implementation process. In addition, many hospitals do not have sufficient security measures in data processing, storage, and transmission, nor do they have sound information auditing and supervision mechanisms. This makes the privacy protection work of hospitals easily overlooked, and management loopholes are difficult to detect and patch in a timely manner. The lack of collaboration among functional departments within hospitals often leads to fragmented information protection work, lacking systematicity and integrity. For example, in terms of data sharing and usage between different departments, hospitals often lack effective permission management and usage restrictions, leading to an increased risk of information abuse or leakage. In addition, hospitals do not handle violations of privacy protection regulations strictly and have not established effective punishment mechanisms, making it difficult to serve as a warning.

4 Countermeasures and suggestions for enhancing patient privacy protection

4.1 Improve the legal and regulatory system and strengthen supervision

In order to effectively protect patient privacy, it is necessary to first improve the relevant legal and regulatory system. At present, although China has the Personal Information Protection Law and the Cybersecurity Law, the specific provisions for privacy protection in the medical field are still insufficient. Therefore, it is necessary to formulate privacy protection regulations specifically for the medical industry, clarifying the legal responsibilities and obligations of medical institutions in collecting, storing, transmitting, and using patient personal information. In addition, the law should also involve cross-border transmission and sharing of medical information to ensure the security of patient privacy on a global scale. Strengthening the supervision of the medical industry is also crucial. Regulatory agencies should conduct regular privacy protection checks to ensure that hospitals and medical institutions comply with relevant laws and regulations and implement privacy protection measures. Establish and improve evaluation and feedback mechanisms for privacy protection, regularly evaluate the effectiveness of privacy protection work, and revise and improve laws based on actual situations. At the same time, the punishment for illegal activities should be increased, the cost of illegal activities should be raised, and a strong deterrent against illegal behavior should be formed. Through the implementation of these measures, the level of patient privacy protection can be effectively improved from a legal perspective, and the risk of privacy leakage can be reduced.

4.2 Strengthen security measures for information technology

With the continuous advancement of informatization, the information technology system of medical institutions plays a crucial role in ensuring patient privacy. In order to strengthen patient privacy protection, hospitals should continuously update and improve information technology security measures to ensure the stability and security of the system. Firstly, hospitals need to adopt advanced data encryption technology to ensure that patient information is always encrypted during transmission and storage, preventing information from being stolen during data exchange. Secondly, it is necessary to strengthen the construction of firewalls and intrusion detection systems in information systems, conduct regular security vulnerability scans, promptly patch possible security vulnerabilities, and prevent external attacks. Hospitals should also adopt multiple identity authentication technologies to ensure that only authorized personnel can access patient information and prevent internal personnel from abusing their privileges. In addition, hospitals should conduct regular cybersecurity drills to enhance the ability of medical staff to respond to information security threats. The backup of information systems is also an important protective measure. Hospitals need to regularly perform data backups and set up disaster recovery mechanisms to ensure that data can be quickly recovered in the event of network attacks or

system failures, avoiding information loss or leakage.

4.3 Enhance the awareness of privacy protection among medical staff

Medical personnel are a key link in protecting patient privacy, but many privacy breaches are caused by the unintentional negligence or intentional disclosure of medical personnel. Therefore, it is crucial to raise the awareness of privacy protection among medical personnel. Hospitals should regularly organize privacy protection training to ensure that medical staff fully understand the importance of privacy protection and relevant laws and regulations, and clarify their responsibilities and obligations. In addition, training should not be limited to onboarding training for new employees, but should also provide regular retraining opportunities for all medical staff to ensure that they are always aware of new changes and requirements in privacy protection. Medical personnel should strictly abide by the principle of patient information confidentiality in their work, and avoid unauthorized access to patient privacy information. Hospitals can establish a dedicated privacy protection committee responsible for regularly checking the implementation of privacy protection by medical staff, and providing consultation and guidance on privacy protection for medical staff.

4.4 Improve the hospital's privacy protection management system

The privacy protection management system of hospitals is the cornerstone of ensuring patient privacy and safety. In order to improve the level of patient privacy protection, hospitals should establish a sound management system for privacy protection, clarify the responsibilities and operational procedures of each link and department in patient privacy protection. Firstly, hospitals should establish detailed privacy protection policies, specifying specific requirements for data collection, storage, transmission, and use, to ensure that medical staff can operate according to standardized procedures. Secondly, hospitals should implement hierarchical management of sensitive data, set different levels of data access permissions, and ensure that only necessary staff can access patients' sensitive information. Hospitals should also establish an information leakage monitoring mechanism, regularly check system logs and data usage, and promptly identify potential leakage risks. In addition, hospitals should establish an emergency response mechanism for information leakage and develop clear emergency plans for information leakage.

5 Conclusion

With the advent of the information age, patient privacy protection has become an important issue that urgently needs to be addressed in medical management. This article analyzes the current situation of patient privacy protection in medical management, reveals deficiencies in laws and regulations, technical means, management systems, and awareness of medical personnel, and points out the main sources of privacy leakage risks. To effectively address these challenges, this article proposes a series of measures, including improving laws and regulations, strengthening information technology security, enhancing healthcare workers' awareness of privacy protection, and improving hospital management systems. By implementing these measures, not only can the level of patient privacy protection be improved, but patients' trust in medical institutions can also be enhanced, promoting the healthy development of the medical industry. Future research should focus on more refined privacy protection technologies, the implementation of laws, and cross industry collaboration mechanisms to meet the increasingly complex needs of medical management.

About the Author

Xiran Feng is an undergraduate student whose research focus is clinical medicine.

References

- [1] Tian Han, Wu Jinping, Zhang Yan, etc Three party evolutionary game analysis of patient privacy protection in surgical live streaming [J]. Chinese Medical Ethics, 2025, 38(1): 123-130.
- [2] Liu Songtao, Liu Mei, Lu Jun Characteristics and Protection Measures of Patient Privacy in Clinical Internship of Infectious Diseases [J]. Continuing Medical Education, 2024, 38(8): 148-151.
- [3] Li Ning, Yang Mingjing, Li Yuxi Data sharing and privacy protection of colorectal cancer from the perspective of medical ethics [J]. Chinese Journal of Medical Ethics, 2024, 37(7): 785-790.
- [4] Zhang Libing, Wang Yang A correlation study on the awareness of patient privacy protection and humanistic care quality among operating room nurses [J]. Health Vocational Education, 2023, 41(6): 89-92.
- [5] Gao Xing, Hong Zhixuan Preliminary exploration of patient privacy protection in health communication activities[J]. News Frontier, 2022(24): 65-66.