Research on the Influencing Factors and Improvement Strategies of Doctor-Patient Trust Under the Privacy and Security Perspective of Medical Big Data

Qiwen Chen, Zhifang He*
1322096225@qq.com, *Corresponding author: 240185357@qq.com

Jiangxi University of Chinese Medicine Nanchang, Jiangxi, China

Abstract—Both doctors and patients are the main bodies of medical activities. Therefore, mutual trust between doctors and patients is the basis of medical activities. Previous studies have shown that patient privacy leakage is one of the important influencing factors causing doctor-patient distrust. However, there are few studies on the influencing factors and promotion strategies for doctor-patient trust based on the perspective of medical big data privacy and security. The influencing factors and strategies to improve doctor-patient trust are discussed in this study from the perspective of medical big data privacy and security. This study combed 158 articles related to medical big data privacy and security. The research results show that the risk of medical big data leakage is mainly manifested in the risk of medical big data collection and application and the risk of medical big data management. Finally, effective methods and suggestions to prevent medical data leakage are further proposed. Moreover, it provides a new research perspective for alleviating doctor-patient conflict, improving doctor-patient relationship and enhancing doctor-patient trust in this study.

Keywords - Doctor-patient trust, medical big data, data leakage

1 INTRODUCTION

In recent years, medical troubles are frequent, and the doctor-patient relationship is increasingly tense. As the core and foundation of the doctor-patient relationship, the lack of doctor-patient trust is an important reason for the tension of the doctor-patient relationship. The medical and health industry is in an era of information disclosure. Decades of development of digital medical records constitute the basis of health big data [1]. With the popularization of intelligent mobile devices, the digitalization of medical devices and the structure of electronic medical records, medical data presents the characteristics of explosive growth [2]. At the same time, the research and development data of pharmaceutical enterprises and other organizations over the years have been gathered in the electronic databases, which has greatly promoted the development of healthy big data. The continuous integration and breakthrough of medical technology and information technology has provided a steady stream of power for the generation of medical data, and also laid a solid foundation for the application and development of big data technology in the medical field. However, while enjoying the valuable information obtained from medical data to inject new vitality into the research in clinical research, health management and public health, it also inevitably brings about the problem of privacy leakage. Patient privacy leakage incidents occur frequently, and the regional big data security situation is not optimistic.

ICICA 2022, December 02-04, Chongqing, People's Republic of China

DOI 10.4108/eai.2-12-2022.2327927

Therefore, how to ensure big data security is a new topic to be solved in the field of information security[3]. Online network environment has problems such as information uncertainty and privacy leakage risk, and these potential risks can hinder the effective communication between doctors and patients[4]. Tang Hong think good doctor-patient communication helps patients and their families to establish the treatment effect of objective, reasonable, realistic expectations, and rational accept the injury caused by medical risk, effective communication can improve the medical staff doctor-patient trust[5], and low communication between doctor-patient quality eventually lead to the relationship deterioration, cause both sides are not satisfied with the process, which lead to the doctor-patient trust decline [6]. At present, China is in a social transition period, and a perfect social credit system has not yet been established. The public trust sense is generally low, and the trust problem between doctors and patients is particularly serious[7]. Therefore, this paper will analyze the causes of medical big data leakage, and put forward reasonable suggestions on the privacy protection and security of medical big data, in order to improve the trust of doctors and patients.

2 DOCTOR-PATIENT TRUST AND THE PRIVACY AND SECURITY OF MEDICAL BIG DATA

2.1 Doctor-patient trust

Doctor-patient trust refers to the belief that the doctor and the patient in the process of interaction, the other party will not make a psychological expected judgment that is harmful to themselves or even harmful to their own behavior. Doctors believe that the patient can actively cooperate with the treatment and understand and respect themselves; the patients believe that the doctor can put themselves in the shoes of the patient's shoes and try their best to recover and escape the pain, leaving each other unprotected[8]. Since the reform and opening up, China has made great achievements. At the same time, it has also faced many arduous social challenges. One of which is that the crisis of doctor-patient trust is becoming prominent. The doctor-patient relationship should be an ethical relationship, and the fundamental attribute of this relationship is equality and trust. Trust cannot be ignored when discussing doctor-patient relationships. Doctor-patient distrust is mainly manifested in the rapid increase of medical disputes and doctor-patient violence. The following is the statistical table of medical disputes in the past five years:

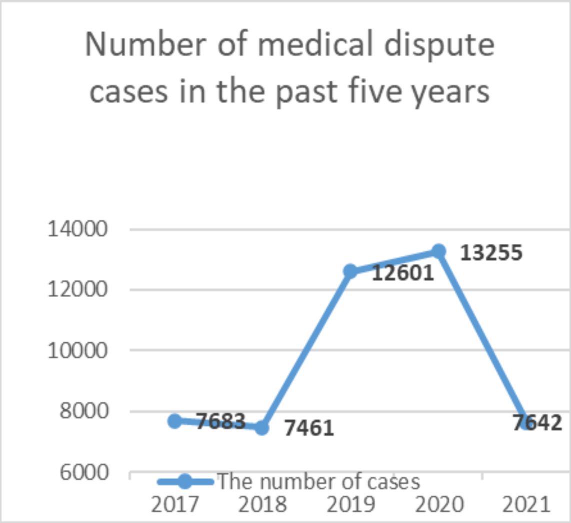

Figure 1 Number of medical dispute cases in the past 5 years

A total number of 1 medical dispute cases in 2021 was 10,746,7,924 fewer than the number of cases in 2020. The overall trend is that after the number of cases in 2018 decreased slightly compared with 2017, it rebounded in 2019 and 2020, and decreased significantly in 2021. Due to the impact of COVID-19, local governments responded to the call of the government and conducted dynamic management. The decline in the number of cases is consistent with the decline in the number of new cases received by local courts due to the epidemic.

2.2 Privacy and security of medical big data

With the extensive application of health care information, massive data sets are generated in the process of medical services, health care and health management. Medical big data platform to the overall data of the health industry data architecture (data model, data, data relationship) set basis and standard, with the corresponding health business data as the entrance, through big data technology, formed in the process of medical treatment, role and business activities, intelligent application, provide timely, predictable, interactive, insight experience, so as to achieve the goal of wisdom of medical treatment. The continuous integration and breakthrough of medical technology and information technology has provided a steady stream of power for the generation of medical data, and also laid a solid foundation for the application and development of big data technology in the medical field. However, while enjoying the valuable information obtained from medical data to inject new vitality into the research in clinical scientific research, health management, public health and other aspects, it also inevitably brings about the problem of privacy leakage. For example, according to the number of security incidents data disclosed by the US Department of Health and Human Services (HHS) Civil Rights Office (OCR), the number of data breaches above the size (500 + items) in the healthcare industry hit a record high in 2020 as shown in the figure:

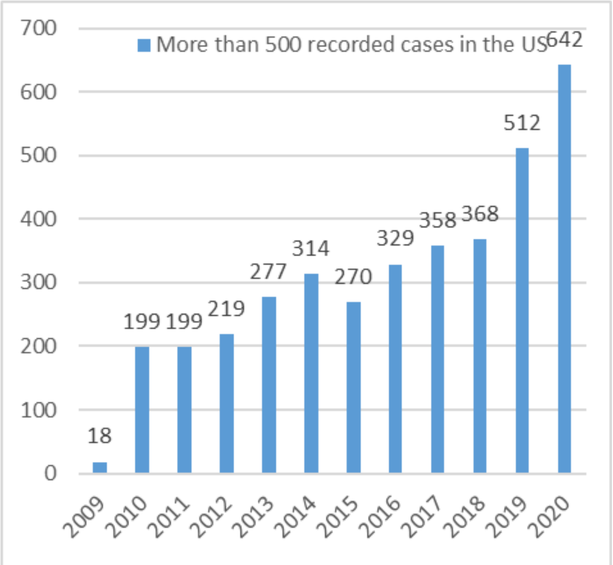

Figure 2 More than 500 recorded cases in the US 2009 to 2020

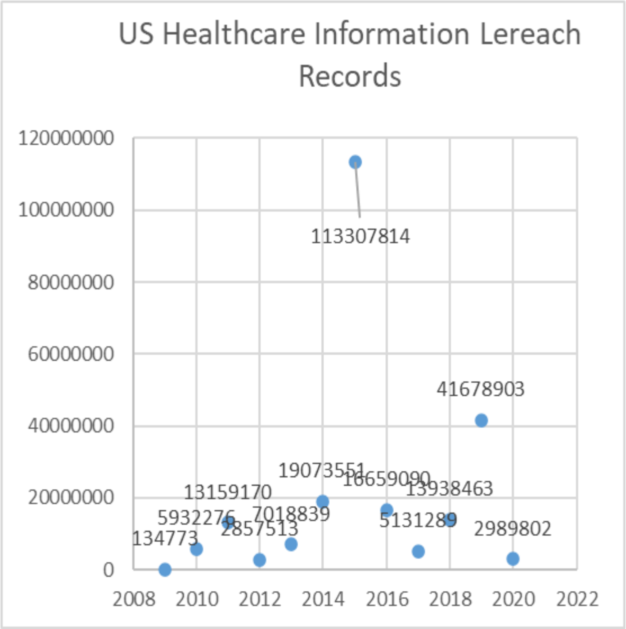

Figure 3 US Healthcare Information Lereach record

In terms of total leaked healthcare records, it ranked third in 2020. There were 29,298,012 medical records that unexpectedly flowed out throughout the year, a 29.71% decrease from 2019. Since October 2009, the healthcare industry has reported a total of 3,705 data breaches involving more than 500 data records, and 266.78 million cases of leaked healthcare records. The number of data breaches reported in the past year was more than double that reported in 2015 and more than three times that reported in 2010.

3 THEORETICAL BASIS

The trust model adopted in this paper was proposed by Johns in 1996[9], which mainly includes 4 phases. Phase 1, absorb potential trustee and relevant information information. Phase 2 involves the processing of the information absorbed in the previous stage, which will lead to the perception of the credibility of the potential trustee. If a potential trustee is deemed to be credible enough, then the principal enters into a relationship of trust. In Stage 3, the relationship is defined as a willingness to assume vulnerability and rely on someone, something to perform as expected. Stage 4 involves the consequences of establishing a trust relationship under specific circumstances. As shown in the figure, after medical big data leakage, patients believe that their privacy is leaked due to trust in doctors, and then absorb information and make decisions of distrust. Therefore, this paper takes the trust process model as the theoretical basis.

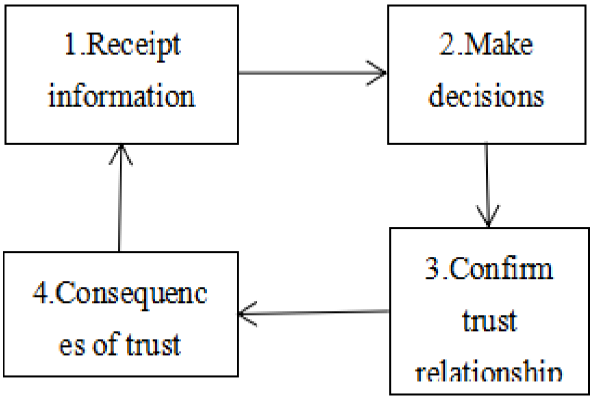

Figure 4 Johns's Trust Model

4 RISK SOURCE ANALYSIS OF THE PRIVACY AND SECURITY OF MEDICAL BIG DATA

Medical big data contains very rich patient information, including a large number of patient records, diagnosis information, expense reimbursement information, etc. In the process of information collection, storage, application and destruction of the medical big data in the cloud environment, the medical data is being used by the users in a roundabout way, greatly increasing the risk of leakage. If the risk source of medical big data can be found and controlled, the risk of data leakage can be greatly reduced. In this study, the risk of medical big data leakage is roughly summarized as the risk of medical big data collection and application, and the risk of medical big data management.

4.1 Medical big data collection and application risk

In the process of medical data collection, the illegal behavior of the organization of privately collecting user information without users 'consent will bring great risks to users' information security. If the medical data collected by the untrusted institutions is transmitted, its untrusted and weak protection measures are likely to be illegally hijacked, causing a risk of privacy leakage.

Data mining of medical information is based on analyzing and processing data, and then obtaining valuable knowledge. When people analyze and mine the massive medical data, this analysis behavior itself poses a threat to the security of the information collected[10].

In the subsequent use of medical data, because in the medical information system, the need of medical data subsequent visitors is more complex, and some institutions access control technology is not very mature, cannot set different access to different visitors, many data collected by institutions will be accessed by managers, if with malicious management access, they may extract and sell users' personal information, in order to seek profits, and make the medical data leakage[11].

4.2 Medical big data management risk

Data management security risk refers to the risk of data leakage caused by poor management in the process of data management. In the era of big data, the data storage side is generally a cloud storage platform. The storage providers and holders of big data are separated, and the cloud storage service providers cannot guarantee that it is fully credible. Users' data is at risk of being peeping or tampered with by untrusted third parties[12].

Due to the large number and diversity of big data, it is difficult to realize the real-time monitoring technology of data at present. Moreover, the regulatory departments lack the corresponding accountability mechanism for those not responsible for data leakage, and fail to play a corresponding warning role, resulting in the increase of the information security risk of data.

In the process of user data destruction, the way is to delete or cover, but the data is not completely destroyed, residual data through equipment hardware maintenance or maintenance and the opportunity to restore data, leading to user privacy data leakage, or in the server maintenance or replacement, data will also face the risk of privacy leakage.

5 SUGGESTION

Patients do not fill in information in untrusted institutions. Public institutions should be selected. For information collection institutions, perfect data encryption work is established in the process of information transmission to prevent data from being illegally hijacked.

Strengthen the research and development and application of data mining protection technology, data mining protection technology: the main purpose is to extract valuable information while not exposing sensitive data[13]. The main data mining privacy protection technology is divided into association rule mining, classification and clustering.

For the data access system, the developed access control technology will first determine who can access it, which is due to the complexity of the involved visitors, and the need to use the technology to set different access rights for different visitors. Secondly, the system uses file layer encryption to ensure that malicious users try to access the data node to directly.

Countries should improve the laws and regulations to protect the personal information privacy security, medical big data is developing rapidly in recent years, but for personal information privacy protection and privacy leakage related laws and regulations is not perfect, lack of when user rights and privacy is violated, the user's privacy and security issues still not due protection.

In the process of data destruction, using physical destruction or inserting scrambled logical destruction, physical destruction is by means of human and external forces to use physical destruction to achieve complete data removal, and cannot be recovered[14]. Logical destruction is to repeatedly write meaningless random data to the data block area ready to be destroyed, to cover and replace the original data, to achieve the purpose of unreadable data, so as to achieve the purpose of data destruction.

Firmly establish legal awareness, the hospital regularly organizes relevant personnel to learn relevant confidentiality laws and regulations, and enhance the legal awareness of all medical staff. When building the medical big data platform, the guarantee of data security is placed in the first place, and a special security team is set up to design the whole security framework, and formulate a standardized safe operation process.

6 CONCLUSION

The lack of doctor-patient trust is an important cause of the doctor-patient tension, and low communication quality between doctors and patients will lead to falling trust between doctors and patients, with the advent of the era of big data, make medical staff to obtain information more spirit, but due to the risk of medical data leakage, make patients may be taboo to doctors, for some hidden disease may conceal, thus affect the communication between doctors and patients. Therefore, this study discusses the risk of medical big data leakage from two aspects of the management process of medical big data and the collection and application process of medical big data, and puts forward suggestions on the corresponding risks to improve the data leakage problem, so as to improve the trust between doctors and patients. This study discusses the influence factors and strategies of improving the trust of medical big data privacy and security, provides a new idea for the study of doctor-patient trust, and further puts forward the effective methods and suggestions to prevent medical data leakage, providing a new research perspective to alleviate the doctor-patient conflict and improve the doctor-patient relationship. However, due to the limitations of some research conditions, this paper still has deficiencies and limitations, which can be further expanded in future studies. This study from the perspective of medical big data privacy and security of doctor-patient trust is mainly from the perspective of patients, the existing medical model, the doctor is in a relatively passive position, the doctor's trust of patients is significantly affected by the patient's trust of doctors, so this paper focuses on the problem of patient trust. However, doctor-patient trust should be mutual in nature, and the analysis of the factors that influence doctors' trust in patients from the perspective of doctors should also get attention. Therefore, the impact of medical big data leakage on the doctor-patient relationship from the perspective of doctors still needs to be explored in the future.

Acknowledgment. The fund of this study is supported by the Doctoral Research Initiation Fund of Jiangxi University of Chinese Medicine (project number: 2020WBRW002), Moderator: Zhifang He.

REFERENCES

[1] Xinrong Zhao, Wei Zhao. Patient Privacy Security Challenge in the context of big data [J]. Digital Medicine in China, 2016,11 (08): 13-15.

[2] Zijing Guo, Yuchuan Luo, CAI Zhiping, Zheng Tengfei. Summary of privacy protection of healthcare big data [J]. Computer Science and Exploration, 2021,15 (03): 389-402].

[3] Hao Ren. Research on big Data security Protection System and Access Control Technology [J]. China Digital Medicine, 2019,14 (02): 52-53 + 87.

[4] Xiaoxiao Liu. Doctor-patient involvement in the online medical community and its impact study [D]. Harbin Institute of Technology, 2019. DOI:10.27061/d.cnki.ghgdu. 2019.000451.

[5] Hong Tang, Wei Liu. Study on the Impact Factors and Countermeasures of Harmonious Doctor-patient Relations [J]. Chongqing Medicine, 2009,38 (24): 3177-3178.

[6] Zhentao Wu, Tailai Wu. Factors influencing patient trust in online health community [J]. Journal of Medical Informatics, 2022,43 (01): 23-29.

[7] Ziying Hong. Research on doctor-patient trust and its dynamic evolution in the Internet Medical environment [D]. Huazhong University of Science and Technology, 2020. DOI:10.27157/d.cnki.ghzku. 2020.001634.

[8] Yifan Li, Xiaoyan Wang, Rui Guo, Guosheng Feng, Jingnan Miao, Jin Hao, Taoxin Mo, Yang Liu. Analysis of doctor-patient trust status and influencing factors from the patient perspective [J]. Hospital Management in China, 2015,35 (11): 56-58.

[9] Johns J L. A concept analysis of trust. [J]. Journal of advanced nursing,1996,24(1).

[10] Yijie Liao, Jing Zhang, Pinghui Li, Rong Jiang, Shanshan Han. Medical big data security risk analysis and Privacy Protection assumption [J]. Chinese Journal of Health Information Management, 2020, 17 (05): 656-660 + 665.

[11] Xiangning Guo, Hongjiang Zhang. Research on the privacy ethics issues of medical big data [J]. Journal of Jinzhou Medical University (Social Sciences edition), 2019,17(03):21-24. DOI:10.13847/j.cnki.lnmu (sse). 2019.03.006.

[12] Binxing Fang, Yan Jia, Aiping Li, Rong Jiang. Overview of Big Data Privacy Protection Technology [J]. Big Data, 2016,2 (01): 1-1813.

[13] Haiyan Kang, Yuelei Ma. Review of the differential privacy protection applied in data mining [J]. Journal of Shandong University (Science edition), 2017, 52 (03): 16-23 + 31.

[14] Hongqian Wang, Peng Wang, Fei Wang, Hao Luo. Ensuring medical big data security and its practice [J]. Journal of Medical Informatics, 2017, 38 (12): 43-47.