WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 4, Number 2, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v4n2.11
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Healthcare Data Privacy Protection Through the Lens of Big Data

Yuexin Pan

School of Sports Engineering, Beijing Sport University, Beijing, 100091, China
pyx666ellen456@163.com

ABSTRACT

In the era of rapid development of big data, there are more and more fields that have a close connection with big data technology, of which the medical field is a particularly important part. Nowadays, citizens reflect that the medical information they had uploaded to the cloud platform has been leaked frequently, even in some regular hospitals and other government-provided platforms, which has aroused citizens' doubts and dissatisfaction. This paper will combine the two perspectives of the field of medical information and big data technology to provide new countermeasures and solutions for solving the problem of medical data leakage from the perspective of big data technology and combining with citizens' awareness of privacy protection.

KEYWORDS

Big data era; Medical data; Privacy protection

1. INTRODUCTION

The arrival of the big data era is like a wheel driving the development of all fields of the era, among which, the combination of the medical field and big data technology is one of the widely concerned combination points. However, with the frequent occurrence of medical data leakage incidents, the privacy of medical data has gradually become the focus of public attention, and citizens have shown general concern about the security and privacy of personal health information. Therefore, this paper analyses the current situation of medical data privacy protection in the context of big data, concludes that there are currently problems of medical data leakage, analyses its impact and proposes countermeasures.

2. BACKGROUND TO THE STUDY

Wang Yuwei, a member of the expert group of the China Chief Data Officer Alliance, once said, "In the era of big data, personal information is not only about personal safety, but also may be related to the public safety of a group." In recent years, with the rapid development of big data technology, the combination of the medical industry and big data is also unstoppable. The way of storing medical information has also changed from paper-based written records to intuitive visual data, which not only improves the accessibility and manageability of data, but also provides the possibility of in-depth analysis and application of data.

At present, it seems that the root cause of the status quo and difficulties faced by medical privacy information is attributed to the shared and specialised nature of medical data, as well as its large scale. Medical data has great potential value in itself, not only for recording patients' medical information,

but also for providing the basis for some medical decisions made by the government. Because of this, the importance of medical data is particularly important to society and individuals. Nowadays, medical privacy data leakage incidents continue to occur, causing dissatisfaction among citizens and interfering with government decisions. Therefore, it is necessary to find out the causes of privacy data leakage and propose corresponding countermeasures.

3. THE CURRENT SITUATION OF MEDICAL PRIVACY DATA LEAKAGE IN THE CONTEXT OF BIG DATA

With the gradual emergence of the Internet + healthcare industry, more and more hospitals nowadays are adopting electronic information to record citizens' healthcare information data, and people have gained access to large-scale healthcare data, such as HIS (Hospital Information System for healthcare services), EHRs (Electronic Health Record System data), LIS (Laboratory Information System data) etc. [1] These data are related to healthcare services, health insurance, personal cases, etc. Therefore, they contain a large number of citizens' personal privacy, even rising to the privacy of the country and society, and once leaked, it will have a great impact on both citizens and the healthcare system. Think about it from another angle, today's society people can not leave the network, can not leave the mobile phone, we use the jittery voice, small red book, wechat and many other social media platforms there is a hidden danger of eavesdropping? If such a hidden danger exists, then our lives are being monitored all the time. At present, domestic scholars' research on the privacy protection of medical data in the era of big data focuses on the leakage of citizens' private data and individuals' awareness of the protection of private information. Therefore, some studies show that the reasons for privacy information leakage are mainly the following three situations:

3.1. Societal Level - Misuse of Healthcare Data Information, Predictions

3.1.1. Data misuse

Data misuse refers to the improper use or processing of personal data without authorisation or in violation of relevant laws and regulations. Such behaviour may violate personal privacy, harm the rights and interests of data subjects, and may cause security problems. Nowadays, the digital management healthcare model is widely implemented, and hospitals upload patients' information to the cloud platform, including electronic cases, consultation records, examination results, etc. However, as this private information have certain potential value, data abuse is common, which often affects people's lives. The most common example is that after this private information are stolen by lawless elements, then some health care advertisements and sales calls will keep pouring into daily life. For the elderly who are less capable of distinguishing between them, there is a great risk of being deceived. A German vulnerability analysis and management company found that 600 unprotected servers were exposed to the Internet, and more than 737 million pieces of radiological image data were threatened, involving more than 20 million people and affecting citizens in 52 countries. This included basic information such as gender, occupation and age for most individuals, as well as medical details such as various types of medical history [2].

3.1.2. Data projections

Data prediction is a technique for estimating future trends or events based on historical data and statistical analyses designed to provide a scientific basis for decision-making. To illustrate with examples from our lives, when we are browsing shopping software, data analytics mining techniques can predict what we need in the near future. If an employee of a company has been browsing and searching for a certain drug recently, the platform will predict that the employee is likely to suffer from such a disease. If this information is leaked out and sold to the employee's company by improper means or in the name of the employee, the employee will face the risk of redundancy.

3.2. Individual Level - Citizens' Low Awareness of Privacy Protection

Some scholars investigated some patients' awareness of privacy information in the region through questionnaires [3]. The study shows that there are differences in patients' awareness of privacy protection under different influencing factors. From this we can see that the personal level is the most subjective reason, citizens on the one hand may be too trusting of the security of the medical platform, on the other hand, citizens themselves do not realise the consequences of privacy leakage, obviously the latter is the more important reason, and this is related to their gender, education level, regional distribution and so on.

3.3. Technical Aspects - Weaknesses in the System Itself When Storing Data

Storing data is a complex process and is a critical aspect of information technology designed to ensure the security, consistency and accessibility of data. Big Data in Healthcare [4]. The lifecycle of big data in healthcare is divided into four stages: data collection, storage, sharing, and analysis, which is like "storing information in a warehouse," and vulnerabilities are inevitable in this complex process. Some scholars classify them into interactive leakage and non-interactive leakage [5]. Interactive leakage refers to data leakage during communication and interaction, while non-interactive leakage occurs when data is lost during data transmission within the hospital. From this, we can see that the platform of the healthcare system still needs to be improved, and if the system can be further improved and the weak links in several complex links can be fixed, the risk of privacy leakage can be greatly reduced.

4. COUNTERMEASURES AND RECOMMENDATIONS FOR PRIVACY PROTECTION

4.1. Improve the Corresponding Laws and Regulations

Medical data is extremely private and important because it contains sensitive health information and personally identifiable information. It is not only related to patients' personal privacy rights and interests, but also an important part of medical security. In view of this, the protection of medical data requires great attention and joint efforts of the whole society.

In the report of the 20th Party Congress, the requirement to improve the level of public security governance and strengthen the protection of personal information is clearly stated. This shows the importance the State attaches to the protection of personal information, especially medical data. The state should further strengthen the construction of relevant laws and regulations, for example, through the enactment of special laws to protect the privacy of patients [6]. The State should further strengthen the construction of relevant laws and regulations, such as by enacting special laws to protect patients' privacy. At the same time, the whole society should actively participate in this action and raise awareness of medical data protection. Whenever it is found that an unscrupulous person attempts to hack into the medical system and obtain or leak patients' private data, the relevant authorities should take decisive action to crack down and impose appropriate penalties in accordance with the law.

4.2. Raising Citizens' Awareness of Personal Privacy Protection

The enhancement of the awareness of personal privacy protection should start from both the state and the individual. At the state level, citizens should be continuously educated about the law, so that they can realise the importance of privacy security; at the individual level, citizens themselves should have the ability to distinguish between right and wrong, and the awareness of the protection of personal information should also be further enhanced. For example, they should not disclose their passwords to others or even to hospitals, and they should not sell their own or other people's information.

4.3. Enhancing the Security and Privacy of Platform Access

For the problem of the system itself, the possible steps of information leakage and the existence of loopholes should be identified, and the medical platform system should be further improved within each healthcare organisation and hospital unit to strengthen the protection mechanism - to strengthen the access control of the firewall to the platform and to ensure that only authorised users can access the private information. From the user's point of view, the medical platform can add multi-factor authentication (MFA), such as SMS verification code and facial recognition. Measures such as data backup and regular updates to fix known vulnerabilities can also be implemented.

5. CONCLUSION

As a cutting-edge field of the times, we can use big data technology as a bridge to build a complete and healthy medical big data platform, combine collected medical information with big data technology, and protect medical information from the big data technology link itself to avoid more data leakage incidents in the future, and provide new ideas and methods for the collection and processing of medical data.

REFERENCES

[1] Wang, Q. (2016) Ethical dilemmas and realisation of medical privacy protection in the context of big data era. China Medical Ethics, (04):685-689.

[2] Qi, Y. (2023) Research on privacy protection issues in the context of healthcare big data. Lantai World, (10):99-101.

[3] Ouyang, T., Yang, Y., Shu, J., et al. (2020) Survey on patients' awareness of privacy protection and ethical thinking in the context of health big data. Journal of Chaohu College, (06):91-97+136.

[4] Guo, Z., Luo, Y., Cai, Z., et al. (2021) An overview of privacy protection of healthcare big data. Computer Science and Exploration, (03):389-402.

[5] Chen, B. (2019) Exploration of challenges and countermeasures for medical data privacy protection in big data environment. Information System Engineering, (09):137-138.

[6] Zhang, X. (2022) Research on the legal protection of personal health medical information in the era of big data (Master Dissertation, Henan University of Finance and Economics and Law). https://link.cnki.net/doi/10.27113/d.cnki.ghncc.2022.000224doi:10.27113/d.cnki.ghncc.2022.000224.