WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 4, Number 3, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v4n3.08
Journal homepage: https://wepub.org/index.php/IJCSIT/index

A Review of the Collaborative Development of Large-Scale Medical Information Systems in China Based on Data Security Policy

Chenshuang Tang, Jiawei Pan *, Jun Wu, Zhongcheng Xu

Information Center, Ruijin Hospital Affiliated to Shanghai Jiao Tong University School of Medicine, Shanghai, China

*Corresponding Author: Jiawei Pan

ABSTRACT

Although in recent years China's governments at all levels and medical administrative bodies have attached great importance to the protection of health and medical big data, and taken various measures to promote the standardized use and effective protection of data, however, China's large population base, health care resources allocation has a strong complexity, so health care data show significant high-frequency changes and complex and diverse characteristics, patients are also in the main links of treatment, payment, and so on, the authenticity of the data are very high requirements. In such a special social environment, from the perspective of both theory and practice, to maximize the application of data in the medical information system while trying to reduce security risks, in the background of relative security to achieve the equilibrium of data utilization and data security, which is worth studying.

KEYWORDS

Data security policy; Medical information system; Collaborative development

1. INTRODUCTION

In the 21st century, big data is a product of the digital age, characterized by Volume, Velocity, Variety, and Veracity. As one of the most active fields of big data application, health care has been highly valued by many countries. Throughout the world, countries around the world rely on data to rise rapidly, "Data sovereignty" will become the border, sea defense, air defense after another big game space, it has accelerated the digitization and intelligentization of large-scale medical institutions and raised the attention of countries to medical data, the medical industry has also become a hot field of national internal policy supervision, international capital competition and Technological Breakthrough.

In contrast, in China, the 2024 National Data Bureau, National Health Commission and other departments issued the "Data elements ×" three-year action plan (2024-2026) , in 2022, the State Council published the Action Plan for promoting big data development, and in 2016, the guiding opinions on promoting and standardizing the application and development of big data in health care, it further confirms the status of big data on health care as an important basic strategic resource of the country. In the context of "Healthy China", health care big data is no longer limited to the diagnosis and treatment data of medical institutions, but refers to a large number of data generated or mined to achieve health care and public health goals. At the same time, our country also puts forward the mandatory laws and regulations to ensure the safety of the patient data stored in the large-scale

medical information system, including the guidelines on promoting and regulating the development of health care big data applications, "Opinions on promoting the development of the Internet plus medical health", "Cyber security law", "Data security law", "Personal Information Protection Law", etc., provide high-level legal system support and guarantee for data security construction. At the same time, the data security requirements for the medical system have been gradually refined, for example, the law on basic health care and health promotion, the measures for the administration of National Health and medical big data standards, security and services, and the information security technology health and medical data security guidelines also require the protection of patients' personal privacy.

2. LITERATURE REVIEW

2.1. Domestic Research Findings

The author searched the core journals related to Big Data Security, health care, and network technology in China in recent years, and analyzed specific cases from different perspectives, such as policy interpretation, the following key academic findings were extracted by dividing them into those based on purely technical aspects.

Zhou Dahong et al. (2024), in the article "Construction and implementation of big data security management system of Medical Consortium", constructed a data security management system based on big data of medical consortium, the establishment of data security policy and the application of security technology in the whole life cycle provide an effective path and security policy for the legitimate development of hospital information system.

Zhang Yuqing (2024), based on the research on the status quo of health care data policies and regulations in China and the reference of overseas legislation model, puts forward some countermeasures and suggestions to strengthen the rule of law. This paper proposes to construct and perfect the legal system of health care data, and analyzes and suggests the mode of "Basic Law + Special Law".

Wang Ying (2022) in the article "Medical industry data compliance and data security issues," through a comparative study of the medical industry data-related laws and regulations, this paper analyzes how to collect, use, store and transmit medical data in accordance with the law, and discusses in detail the data security management of the popular Internet hospitals.

Li Lin (2022), in the article of "Security Protection of medical data based on blockchain technology", proposes to use linear discriminant analysis algorithm to complete the extraction process of medical data features, set up a secure isolated area in the hospital's medical data storage database, and encrypt the medical data transmission channel by VPN, in order to realize the security protection of medical data storage, the network terminal equipment and medical database are protected.

Duan ran et al. (2021) independently innovated the design and implementation of the Intelligent Hospital Medical Data Security Exchange platform, which is the first Internet security management platform system in China, it changes the structure and layout mode of the existing security products, makes the functions more comprehensive and perfect than the existing hardware security product mode, and fully realizes the visualization, transparency and intelligent supervision of the data flow and control flow, it represents the development direction of future network information security construction and has epoch-making guiding significance.

Wang Qianchuan (2019) pointed out in "Research on security protection of medical privacy data in 5G Cloud Edge collaborative scenarios" that information security engineers can build 5G network architectures based on mobile medical edge clouds, the use and storage of patient's private information are separated physically, and the private information is classified and encrypted by different algorithms.

Youjinze et al. (2018) focused on IBM Watson Health, a leader in cognitive medical technology, exploring the complexity and severity of online and indirect access to informed consent and individual data privacy protection, with a view to keeping a close eye on the security and privacy of individual data in the context of the ethical nature of medical information itself as a business model for technological innovation in cognitive medicine, the result is "A data security ethical perspective for cognitive medicine in the big data era-a case study of IBM Watson Health".

2.2. Foreign Research Results

According to the search classification of domestic research results, the author searches and selects the following major foreign research results. In 2018, the Health Information Security & Privacy Collaboration (HISPC2) proposed a framework for discussing data exchange scenarios and Privacy Security issues, the discussion of privacy and security in patient care scenarios can be divided into two categories, one is the management strategy of privacy and security, the other is the technology implementation of privacy and security.

As Singh Amit Kumar (2021) points out in his article "Recent trends in healthcare data security for e-health applications", there have been important breakthroughs in the following areas: It includes health data collection based on multi-sensor and intelligent terminal, distributed storage and parallel computing based on cloud platform, real-time processing of dynamic big data and unstructured data processing, the deep integration of multi-variable and heterogeneous data, the learning, reasoning, prediction and knowledge discovery of massive dynamic data, etc.

Fatlawi Hayder K (2021) further refines it and proposes a differential privacy classification model based on Adaptive Random Forest (ARF) in ARF mining medical data stream classification model. The experimental results on 4 medical datasets show that most ARF techniques have more stable performance than the other 6 techniques. Vandana Bharti (2020), in his article "A new multi-objective Gdwcn-PSO algorithm and its application in medical data security", points out that the generated adversarial network (Gans) has become a powerful model in the fields of computer vision, speech and language processing, it can provide important technical support for medical data security.

Kukatlapalli Pradeep Kumar (2024) proposed in his article "Secure approach to sharing digitized medical data in a cloud environment" that patient health information is scattered throughout the hospital environment, Including laboratories, pharmaceuticals, and daily medical status reports. The electronic format of medical reports ensures that all information is available in a single place. However, it is difficult to store and manage a large amount of data. Storing data in a cloud is a cheaper alternative. Through domestic and international searches, it has been found that academic journals or papers related to medical data security are increasing year by year, with 2024 possibly being another peak year for paper publications in this field.

3. RESEARCH AND ANALYSIS

3.1. Research Significance

From a practical point of view, the data related to medical activities, such as life health, medical services, medical care, public health, etc., are in the whole policy life cycle, and the medical data is people's health pursuit, health care needs and big data technologies. For the country, ensuring the data security of large-scale medical information system has become an important measure of a country's comprehensive strength, which is conducive to preventing network intrusion from home and abroad, and maintaining the country's "Data security", even economic, political and social security. In addition, ensuring the data security of large-scale medical information systems reflects the state's high attention to the privacy of citizens and national information security, which is conducive to increasing the public's trust in national policies and strategies and ensuring better implementation. For the

medical industry, ensuring the data security of large-scale medical information system can control the risk of medical industry data security, achieve the balance of data utilization and security, and ensure the healthy growth of the industry. For the general public, ensuring the data security of large-scale medical information system is the basic project to realize "The health of the whole people" and improve people's health, to provide continuous and stable tripartite security for the health care market on the demand side, the supply side and the payer side. In addition, the construction of a safe and efficient medical data network LED and advocated by the state can help the public establish a scientific concept of health and medical big data security, promote the maximum use of health and medical big data, and reduce social risks.

On the theoretical level, the first is that in the context of the gradual introduction of medical data sharing in China, it is necessary to fully learn from foreign experiences and lessons, data collection channels, publicity and communication mechanisms to conduct in-depth research to provide a theoretical basis for new policy formulation. Second, the construction of data model in the medical information system is helpful to strengthen the effect analysis of the policy from the theoretical level, so as to reverse and perfect the establishment of the policy system. Third, from the perspective of personal privacy data, when the sensitivity of medical data and data sharing and sharing model, the possible existence of data errors, data use, such as unclear definition of the impact of the rights of data owners, how can individuals justify their use in terms of policy theory.

In addition, from the perspective of academic innovation, there is no lack of analysis of our country's current health care big data strategic planning, governance status, research status and application status quo, as well as from a more long-term, more professional point of view to propose specific solutions, such as "Hard-and-soft" technology promotion and sharing programs and the use of "Defensive advance" strategy to ensure data privacy security. All these studies have theoretical height and professional reference, but this study will cross the "Pure information" or "Pure medical" field, the two will be cross-sectoral organic combination, it may provide a new way of thinking about the organic balance between medical data collection, privacy security and national big data strategies.

Table 1. Number of relevant documents on a website over the years

Year	2017	2018	2019	2020	2021	2022	2023
Chinese	168	201	231	301	308	381	379
Foreign languages	7	19	36	40	26	29	45

3.2. Research Objectives

Specifically, this review aims to analyze the status quo of data security protection of domestic-based large-scale medical information systems, including policies, laws and regulations, technical means, personnel training, etc., and based on the domestic and foreign large-scale medical information system data protection strategy and protection focus, then it puts forward how to establish our country's large-scale medical information system data protection relative security concept and specific solution strategy (also from the legal supervision, personnel training, propaganda and education, key data protection, technology research and development and other aspects of health care big data security risk prevention and control system), in this way, patients in our country can share their treatment experience on the open website platform, doctors can provide consultation service on the website, and make the policy and information system benefit and develop for the better, provide a better experience for both doctors and patients. The ultimate goal of this study is to maximize the application of data while minimizing safety risks, to achieve a balanced state of medical data utilization and patient data safety in the context of relative safety, and to promote health in the medical industry, efficient development.

In addition, attempts can be made to break down the cognitive barriers between information technology, policy planning and social management and to find a balance between the three, namely,

to make the superstructure of the state more acceptable to the people with the support of technological means, to understand, identify, and bring true technological well-being, health well-being to the people, so as to push back the development of technology and the implementation of policies. Finally, I hope to make the best use of my work experience in medical institutions and years of professional knowledge in the data security industry, from the theory, technology, practice and many levels of professional advice, it can also provide individuals with case experience in their field of study and important guidance for their future career.

3.3. Possible Research Directions

How to ensure data privacy security from the aspects of talent system construction, technology R & D promotion (emphasis), law enforcement, policy support and supervision, etc., to help achieve the goal of "Health + big data". Here are some possible ways to think about this:

In the planning stage of the medical information system, how to incorporate the current policy of data security and the development trend in a number of years into the system planning and design in a forward-looking manner, so as to ensure that the information system can adapt to the changes of the policy requirements for a longer period of time after planning.

In the development stage of medical information system, how to ensure the implementation of the detailed standards of data security, reduce the logic loopholes of information system, and ensure the implementation and reliability of data security policy at the software level.

In the stage of operation and maintenance of medical information system, how to respond to the real-time requirement of data security policy and how to change the information system when there is a policy gap, so as to support the long-term operation and maintenance of the information system.

Mechanisms to ensure compliance with data security policies during the decommissioning phase of medical information systems to enable data destruction to reduce the risk of data leakage exposure.

The contents that are included in the scope of consideration include the foundation of our country's current health care big data strategic planning, governance status quo, research status quo and application status quo, and prove the social value, strategic value and economic value of health care big data.

On the whole, this paper has demonstrated the necessity, pertinence and feasibility of this research from the healthy environment of China and the practical significance of the development of large-scale medical information system.

3.4. Possible Findings

The "Healthy China" strategy has raised the bar for policy making in China and deepened the meaning of big data on health care. Health care big data in the context of "Healthy China" breaks through the limitations of previous medical professional institutions' diagnosis and treatment data, covering health care, public health and other areas affecting the health of the whole population. It is a realistic opportunity and historical mission for our country to develop the health medical big data industry, which must be unswervingly pushed forward, technology, talent, funding, equipment, legal supervision can't fully keep up with the pace of industrial development, can't fully guarantee data security, health and medical big data collection, storage, trading, processing, application of the various links of security risks will exist for a long time. So, it's possible to do the following:

By using the experience and lessons of foreign countries for reference, this paper provides a theoretical basis for new policy-making of data security protection in medical field of our country, and helps to perfect the establishment of policy system.

We will encourage the health care industry to fill information technology gaps, improve relevant laws and regulations, take a more pragmatic approach to security issues, and take the responsibility of protecting the absolute security of big medical data.

To guide the public to establish a scientific concept of medical data security, to raise awareness of personal data protection, and to enhance information on national data security protection capabilities and professional service capabilities of the medical profession, improve personal security and well-being.

To sum up, smart medicine is the direction of health care industry development, big data is the foundation of smart medicine, only grasp the development of big data to grasp the future of health care industry. The development of health care big data is bound to face the related problems such as security and privacy protection, but under the premise of taking corresponding preventive measures, the development of health care big data technology has brought more "Advantages" than "Disadvantages" to the national health. How to deal with these problems and challenges in the development of Big Data Technology for health care is a new test in the digital economy era. We can't avoid these problems by rejecting the development of technology, we have to use more courage and caution to meet these challenges.

4. SUMMARY

Take That observation back to the medical profession. After years of information construction, large-scale medical institutions have also built numerous medical information systems, a medical management system based on HIS, an electronic medical record system based on EMR, and an image archiving and communication system based on PACS are formed, and laboratory information system based on LIS, etc. In the whole life cycle of related information system, it is necessary to design, implement and put into operation synchronously for the coordination of data security policy. However, it is not difficult to find that with the rapid development of health care big data industry and the persistent influence of infectious diseases such as COVID-19, the security risks of health care big data are becoming increasingly prominent, this is reflected in internal problems (shortage of professionals, barriers to technology promotion, security of information storage, trading, processing media, construction of data management database, desensitization granularity and effect, insufficient data security planning, excessive risk exposure of full-volume circulation, lack of detailed policies and supervision on the destruction of obsolete data in old systems) and external problems (all kinds of incidents endangering data security emerge one after another, the sources of risks are increasingly widespread, and the methods of infringement are increasingly sophisticated). Along with the "Internet + medical" makes the situation of health care big data security protection more serious, the medical profession puts forward to the health care big data security protection more urgent need, large-scale health information systems also need to be reformed.

CONFLICTS OF INTEREST

Author reports no disclosures.

ACKNOWLEDGEMENTS

Thank you very much to all the researchers and friends around me, who have provided a lot of reference and guidance for this study.

REFERENCES

[1] Seventeen departments including the National Data Bureau jointly published the full text of the "Data elements ×" three-year action plan (2024-2026) [J]. Automation Expo, 2024, 41(01): 2.

[2] Circular of the State Council on issuing the Action Program for promoting the development of big data [EB/OL]. (2015-09-05) [2018-03-12]. Http://www. Gov.cn/Zhengce/content/2015-09/05/content 10137. HTM.

[3] The State Council general office has issued the "Guiding opinions on promoting and standardizing the application and development of big data in health care"[EB/OL]. (2016-06-24) [2018-03-12]. Http://www.gov.cn/xinwen/2016-06/24/content. HTM.

[4] "Opinions on promoting the development of "Internet + Medical Health""[EB/OL] was issued by the State Council General Office. (2018-04-28) [2018-03-12]. Http://www.gov.cn/xinwen/2018-04/28/content. HTM.

[5] Zhou Dahong, Huang Yifan, Wang Hongqian, etc. Construction and implementation of a big data security management system for the medical consortium [J]. Journal of Health Informatics, 2024, 45(06): 68-73.

[6] Kumar P K, Prathap R B, Thiruthuvanathan M M, et al. Secure approach to sharing digitized medical data in a cloud environment [J]. Data Science and Management, 2024, 7 (2): 108-118.

[7] Zhang Yuqing. The status quo of health care data policies and regulations in China and the reference of extraterritorial legislation model [J]. Journal of Health Informatics, 2024, 45(02): 26-31.

[8] Skipper. Study of learning models for healthcare data characteristics [D]. Huazhong University of Science and Technology, 2017.

[9] Tao Xuejiao, Hu Xiaofeng, Liu Yang. Review of Big Data Research [J]. Journal of systems simulation, 2013, 25(S 1): 142-146.

[10] Yan Yan, Qin Xingbin, Fan Jianping, Wang Lei. Review of healthcare big data research [J]. E-science, 5(06), 2014:3-16.

[11] Yu Guopei, Bao Xiaoyuan, Huang Xinting. Types, nature and issues of health big data [J]. Journal of Health Informatics, 2014, 35(06): 9-12.

[12] Wang liming. On the legal protection of the right of personal information-focusing on the division between the right of personal information and the right of privacy [J]. Modern law, 2013, 35(04): 62-72.

[13] Zhang Yujie. Healthcare data flow and governance change in public health risk [J]. Hebei law, 2020, 38(06): 51-60.

[14] Zhang Xinbao. From privacy to personal information: the theory and institutional arrangement of reweighing interests [J]. Chinese law, 2015, (03): 38-59.

[15] Xu Jing. A study of China's population development and health under the new economic normal [A]. Chinese Association of Soft Science Research, Chinese soft science collection, 2019 [C]. Beijing: China Association of Soft Science Research, 2020.32-39.

[16] Health care big data in depth [J]. Software and integrated circuits, 2019, (10): 70-73.

[17] Li Houqing, Yin Cui Qun, Fan Jinyan. China Health Care Big Data National Strategic Development Study [J]. Library, 2019, (11): 30-37.

[18] Cai Xiaoheng A Review of Xi Jinping's Important Discourse on Healthy China [J] Journal of the Yunnan Provincial Party School of the Communist Party of China, 2020, 21 (02): 56-59.

[19] Cui Wenbin, Tang Yan, Liu Yongbin. Theoretical and practical exploration of the construction of intelligent hospital [J]. Chinese hospitals, 21(08), 2017:1-4 + 8.

[20] Chen Jin, Xu Bingnan. Health big data security technology [N]. Health, October 13, 2018(003).

[21] Ren zeping, Xiong Chai, Luo Zhiheng. It is high time to start the "New infrastructure" [J]. China finance, 2020, (06): 77-78.

[22] Liu Chunfu, Chen Hongmin. On the relative safety of big data protection in health care [J]. Journal of Zhejiang University (medical edition), 2018, 47(06): 563-576.