Medical Management Advances 2025 1(1):13-18
https://www.auberpublishing.com/index.php/MMA/index
E-mail: editorialoffice@auberpublishing.com

Review

An analysis of network security and protection strategies in hospital informatization

Wen Chen, Nan Mao, Jie Zhu*

School of Engineering and Technology, Nanchang Vocational University, Nanchang 330013, China

Abstract
At present, the continuous development of information technology has made hospital informatization a key driving force for improving the quality and efficiency of medical services. The rapid formation of smart hospital systems, facilitated by the deep integration of information and IoT technologies, has significantly enhanced the service capabilities of hospital information platforms and established a comprehensive security barrier for existing network infrastructures. However, alongside advancements in informatization technologies, network security challenges have become increasingly prominent, posing major obstacles to the progression of hospital informatization. This paper highlights the critical importance of network security in hospital informatization, analyzes current security challenges, identifies the factors influencing network security issues, and explores the risk points associated with hospital informatization. Furthermore, it proposes a series of targeted protection strategies aimed at providing valuable guidance and reference for hospital information security management practices.

Keywords: Hospital informatization; network security; protection strategies

1 Introduction

In recent years, continuous development and innovation in information technology have significantly improved hospital information systems. Simultaneously, technologies such as mobile internet devices, network technologies, and cloud computing platforms have matured, increasingly integrating into hospital information networks. This integration has greatly enhanced the efficiency and quality of clinical diagnosis and service delivery in hospitals. However, it has also introduced new challenges to information security within hospitals.

To advance hospital informatization systems rapidly, it is essential to enhance the protection of internal hospital information networks, ensuring that the safety requirements of hospital informatization are met [1]. In this context, strengthening awareness of network and system security, addressing potential vulnerabilities and risks, and implementing proactive and effective measures are crucial for the timely prevention and control of security issues. Additionally, hospitals must establish and optimize operational standards, network environments, and technical support systems for information security. They should strictly manage information security processes, details, and workflows to enhance the protection of internal hospital information data. Such measures provide reliable managerial, technical, and operational safeguards for building a stable and secure information platform.

2 The Critical Importance of Network Security in Hospital Informatization

2.1 Ensuring the Efficient Operation of Medical Services

The stable operation of hospital informatization systems forms the foundation for the efficient delivery of medical services. For instance, electronic medical record systems ensure the accuracy and completeness of patient information, enhancing diagnostic precision and work efficiency. Appointment systems significantly reduce patient waiting times, streamlining outpa-

***Correspondence**
Jie Zhu, School of Engineering and Technology, Nanchang Vocational University, Nanchang 330013, China
E-mail: 2691475834@qq.com

tient service processes, while telemedicine transcends geographical barriers to enable scientific allocation of medical resources. The effective functioning of these systems relies on robust network security measures. Any form of cyberattack could lead to system paralysis, data loss, or unauthorized access, severely threatening the continuous and stable delivery of medical services.

2.2 Protecting the Sensitivity and Privacy of Patient Data

Medical data often contains highly sensitive information, including patients' personal privacy, detailed health conditions, and treatment records. Any data breach could result in severe violations of patients' privacy rights, potentially triggering a trust crisis within society and causing irreparable damage to the hospital's public image [2]. Consequently, reinforcing network security measures to ensure the safety and privacy of patient data is a fundamental social responsibility and obligation for hospitals during the informatization process.

2.3 A Foundation for Scientific Research and Innovation

Medical big data, a valuable resource for medical research, plays a pivotal role in cutting-edge fields such as drug development, disease prediction modeling, and the formulation of precision medical strategies. Through in-depth analysis and mining of these massive datasets, researchers can uncover the evolution of diseases, providing scientific evidence for clinical decision-making. However, all such exploratory and innovative actions depend on the secure and reliable storage and integrity of data. Therefore, strengthening network security to safeguard the secure storage and efficient utilization of medical big data is a cornerstone for advancing medical technology and fostering continuous innovation [3].

3 Factors Influencing Network Security in Hospital Information System Development

3.1 Technical Factors

Hospital network systems typically integrate multiple components such as servers, network devices, client terminals, software systems, routers, communication lines, and storage facilities. Due to the late start of hospital information system development in China, a lack of experience has led to various challenges in network security management. These challenges include system maintenance and inspection, physical environment management, data protection, and operating system security.

One key issue stems from the limited capabilities of firewalls, which are often inadequate in preventing bypass intrusions and internal security threats. While firewalls can issue attack alerts and provide IP tracking, they are less effective in preventing malicious activities like data tampering and theft. Additionally, many hospitals lack standardized management of MAC and IP addresses, allowing administrators to easily modify address information. This makes it difficult to trace responsibility when security incidents occur.

The application of antivirus software also faces challenges due to the large number of hospital workstations and the frequent turnover of users. Comprehensive deployment, including software installation, regular scans, patching vulnerabilities, and updating virus definitions, is often infeasible. This weakens the overall security framework, making it difficult to achieve desired safety objectives.

3.2 Human Factors

(1) Awareness and Expertise Deficiency:

Human error plays a dominant role in the daily operation and maintenance of hospital networks. Many hospitals lack sufficient awareness of information security and do not prioritize it adequately. This leads to a shortage of skilled professionals in security management. Medical staff generally lack basic knowledge of cybersecurity, and hospitals often do not have a formal and specialized security management team. Consequently, weak overall security awareness and inefficient operations prevail [4].

When network security incidents occur, hospitals frequently struggle to respond swiftly and effectively due to inadequate expertise, severely compromising the effectiveness of security management.

(2) Operational Errors:

Errors or negligence by staff can result in system breaches that pose significant threats to hospital operations. Such risks, arising from improper actions, are an essential aspect of hospital network security management that cannot be ignored.

(3) Unsafe Internet Activities:

When system operators download software or browse websites on public networks, they may inadvertently introduce malware or viruses into the hospital network. This greatly increases the risk of virus attacks and highlights another critical issue requiring urgent attention [5].

If not effectively controlled and mitigated, these human factors can have a profound negative impact on hospital information system development, potentially leading to the leakage of sensitive hospital data and significant financial losses.

3.3 Viruses

Computer viruses pose a severe threat to network security. With their high concealment, extensive propagation, and activation mechanisms, viruses can infiltrate computer networks, slowing system performance, causing crashes, and resulting in data loss.

Hospitals, as data-intensive and highly interactive platforms, are particularly vulnerable. If viruses enter the system due to improper operations, they can spread rapidly across network nodes, causing widespread disruption. Furthermore, the stealthy nature of modern viruses makes them difficult to detect and remove using existing antivirus tools.

Source code-based viruses are especially dangerous as they directly target and disrupt application systems. With continuous advancements in virus technology, their ability to embed, hide, and evade detection has significantly increased, posing even greater challenges to network security defenses.

3.4 Equipment Factors

The foundation of hospital information systems lies in the deployment and normal functioning of hardware devices. However, in practice, some equipment shows signs of aging or delayed updates, making it incompatible with rapidly evolving network and software technologies. This mismatch limits the performance of the equipment and introduces security risks, such as operational failures or data loss, which threaten daily hospital operations.

When hardware is incompatible with current network systems and software applications, the likelihood of equipment damage increases, exacerbating network vulnerabilities. Additionally, shortcomings in MAC and IP address management further undermine the effective implementation of security measures, potentially rendering the hospital's carefully designed security framework ineffective [6].

4 Risk Points in Hospital Network Security

4.1 Information System Security Vulnerabilities

Many hospitals in China lack robust awareness and measures for data security. As a result, large volumes of unencrypted data are left vulnerable to attacks. Hospitals often rely on basic built-in firewalls, which offer limited protection, and lack advanced firewall systems or intrusion detection mechanisms [7]. This makes them susceptible to malicious attacks, including data theft and unauthorized access.

The increasing openness of hospital network systems, driven by digital transformation in healthcare, has further exposed medical data to significant risks. Hackers and other malicious actors can exploit these vulnerabilities to gain control over services and steal sensitive information.

4.2 Risk of Patient Data Leaks

Patient information constitutes a substantial portion of hospital medical data. If leaked, such information can have severe repercussions on patients' lives. The causes of data breaches are diverse, including malicious attacks by hackers, negligent staff practices, and security loopholes in third-party service providers.

As hospitals deepen their reliance on information systems, collaboration with third-party entities requires thorough evaluation of their credibility and technical capabilities. Failure to do so could introduce potential risks to the security of hospital systems.

4.3 Risks in Data Sharing and Application

The value of medical data lies in its application and transformation. As the volume of hospital data continues to grow, so does its range of applications. However, privacy concerns remain critical, as much of this data pertains to patients [8].

If hospitals do not prioritize data security during utilization, they face serious risks. Improperly anonymized data can be easily leaked during sharing, and even well-processed data can be compromised if clear security guidelines and operational protocols are absent.

5 Strategies to Address Network Security Issues in Hospital Information System Development

5.1 Establishing a Robust Network Security Framework

To address the network security challenges in hospital information system development, a thorough analysis of influencing factors must be conducted, followed by a systematic plan to strengthen security measures. These measures require support from a well-defined institutional framework.

First, hospitals must comprehensively evaluate their network infrastructure, identifying potential security threats through meticulous inspection and monitoring. Security protocols and emergency response plans should be formulated based on the system's structure and specific risk points, ensuring strict adherence to these protocols [9]. Regular audits of system operations, along with routine risk assessments, are necessary to proactively mitigate emerging threats. Assigning clear responsibilities during each phase of system development and enhancing oversight can effectively control and reduce network risks.

Specific measures include implementing advanced protection strategies for wireless ports to block unauthorized signals, creating a secure environment for network users, and strengthening authentication protocols. For instance, patients registering or logging into the hospital website must go through rigorous security checks to ensure the authenticity of their personal information, thereby reducing identity theft risks. Moreover, setting up tiered access permissions and employing multifactor authentication methods, such as passwords, can enhance data security. Encrypted data transmission between hospital departments is crucial to prevent breaches caused by weak firewall defenses. Establishing comprehensive management systems will facilitate regular inspections, evaluations, and effective oversight of hospital network platforms.

5.2 Enhancing Network Security Isolation

Safeguarding internal hospital data is a critical aspect of network security, and network isolation plays a pivotal role in this effort. Security strategies should be tailored to the unique needs of each department. For example, in the finance department, maintaining confidentiality of critical information and ensuring smooth data management processes is essential. Adjusting administrative permissions and implementing strict access controls is necessary to protect sensitive data.

Hospitals should integrate their local area networks (LANs) with key systems such as national social insurance databases and Hospital Information Systems (HIS). Security management must also extend to hardware infrastructure, including hard drives and network cables, ensuring the integrity of the hospital's information systems. Advanced network designs and isolated system modules can further enhance security and operational efficiency [10].

Technical personnel should continuously upgrade their skills to keep pace with technological advancements, ensuring the implementation of state-of-the-art security measures to support the sustainable development of hospital information systems.

5.3 Deploying Effective Antivirus Software

Effective network security hinges on robust software management. Deploying versatile antivirus software is a fundamental step to monitor and regulate system performance. These tools are essential for real-time scanning, detecting, and neutralizing threats to maintain efficient data transmission [11].

Antivirus programs can identify potential threats by matching data against an internal virus database, preventing security breaches. These programs operate continuously, monitoring system performance and issuing alerts in case of anomalies. Regular updates to antivirus software are crucial for combating emerging data threats, ensuring the hospital's digital environment remains secure and operational.

5.4 Backing Up System Data

Data backup is an essential component of hospital network security management. Understanding the limitations of computer storage and performance is critical. Data loss due to hardware failures or system instability can significantly disrupt hospital operations.

To mitigate these risks, hospitals should adopt strategies such as uploading data to cloud platforms and enabling automatic synchronization for backup. Cloud storage ensures that critical data can be recovered quickly in case of hardware failures, safeguarding data accuracy and completeness [12]. This approach not only enhances data security but also ensures stable and efficient system operations.

5.5Strengthening Hardware Security

Securing hardware infrastructure at the physical level is vital. Key measures include:

•Implementing physical controls for hardware equipment and optimizing password authentication processes.

•Housing servers and associated equipment in lockable cabinets with designated personnel managing access. Installing surveillance cameras to cover all areas ensures comprehensive monitoring.

•Ensuring compliance with environmental standards, such as anti-static flooring and advanced lightning protection, to provide a stable operational environment. Dual power supply systems should also be deployed to maintain continuous power for critical components [13].

These measures protect against information theft and ensure smooth operation of hospital systems, supporting overall functionality and service delivery.

5.6 Enhancing Staff Competency in Network Security

The rapid advancement of information technology necessitates the cultivation of skilled professionals in network security. Hospitals must focus on attracting and training talent to build a competent network security team capable of identifying and addressing potential vulnerabilities.

Regular training sessions for all hospital staff are essential to enhance their technical proficiency and awareness of cybersecurity practices. Staff should be trained to safeguard sensitive information, avoid high-risk websites, and remain vigilant against potential threats such as malware or phishing attacks. These efforts help maintain data integrity and reduce the risk of breaches [14].

5.7 Developing Tailored Emergency Response Plans

Given the unpredictable nature of cybersecurity incidents, hospitals must prepare detailed and actionable emergency response plans to minimize disruptions. These plans should be informed by a comprehensive analysis of past incidents, potential risks, and their impact [15].

The response plan should outline clear procedures for each department, especially those providing direct patient care, and include an effective command structure. The plan must also be adaptable to other emergencies, ensuring a high level of preparedness.

5.8 Increasing Financial Investment in Cybersecurity

The sustainable development of hospital information systems relies on robust network security measures, which require significant financial investment. Procuring advanced software and hardware, such as antivirus programs and secure authentication systems, is essential for maintaining system security.

For critical systems, implementing dual-server backups ensures business continuity and data integrity during failures [16]. Hospitals should also invest in advanced identity verification technologies, such as USB security tokens, to prevent unauthorized access and data tampering. Adequate funding ensures the implementation of these measures, reinforcing the hospital's cybersecurity infrastructure.

By integrating these strategies, hospitals can effectively address network security challenges, ensuring the safe and efficient operation of their information systems.

6 Conclusion

With the continuous advancement of information technology, hospital information system development has become a key factor in improving the quality and efficiency of medical services. Strengthening network security in hospitals is not only essential for ensuring the efficient operation of medical services and safeguarding patient data privacy but also serves as a critical foundation for driving innovation and progress in medical technology.

Hospitals must establish a comprehensive network security framework, enhance network isolation and protection measures, deploy effective antivirus software, and focus on upgrading the security levels of hardware devices. At the same time, efforts should be made to improve the professional expertise of hospital staff, develop emergency response plans for network security incidents, and increase financial investment in the field of information security.

Looking ahead, as hospital information systems continue to evolve, network security challenges will persist and grow more complex. Hospitals must adapt to these emerging security threats, continuously optimize and refine their network security systems, and ensure the secure and stable operation of their information platforms.

Only by taking these measures can hospitals better

serve patients, ensure the privacy and integrity of medical data, and contribute to the sustainable and healthy development of the healthcare industry.

Acknowledgments

Not applicable.

Conflicts of Interest

The authors declare no conflicts of interest.

Author Contributions

Conceptualization: J.Z.; Writing-original draft: W.C. and N.M.; Writing-review and editing: W.C. and N.M. All authors have read and agreed to the published version of manuscript.

Ethics Approval and Consent to Participate

No ethical approval was required for this review article.

Funding

This research received no external funding.

Availability of Data and Materials

The data presented in this study are available on request from the corresponding author.

Supplementary Materials

Not applicable.

References

[1] Shen ZW. Discussion on network security management and protection in hospital information construction [J]. *Wireless Internet Science and Technology*, 2021, 18(22):33-34.

[2] Lu Y. The Maintenance Strategy of Network Security in Hospital Informatization Constructio[J]. *Telecom Power Technology*, 2020, 37(4):143-144.

[3] Liu FR. Data Security Strategies for Hospital Informatization Construetion [J]. *Journal of Medical Informatics*, 2010, 31(11):31-33.

[4] Ye P. Risks in the Hospital Informatization Construction and the Data Safe Management [J]. *Journal of Medical Informatics*, 2010, 31(6):21-23.

[5] Long ZY, Chen J, Yang GP, *et al.* Network security and protection of hospital information construction [J]. *Medical Education Management*, 2021, 7(6):675-679.

[6] Xiao Y, Bai WB, Sun J, *et al.* The Course and Prospect of Network Security Construction of Traditional Chinese Medicine Hospitals in China [J].*Journal of Medical Informatics*, 2021,42(10):1-5,10.

[7] Yu M and Fang GW. Discussion on the Construction and Safety of the Network Information System in the Specialized Hospital [J]. *China Medical Devices*, 2015, 30(11):71-72,70.

[8] Xing Y. Thought of hospital archives informatization security management [J]. *Chinese Journal of Integrated Traditional and Western Medicine in Intensive and Critical Care*, 2021, 28(3):369-370.

[9] Wei MY, Cui WB, Wang S, *et al.* Risk analyses and supervision strategies of internet hospitals [J]. *Health Development and Policy Research*, 2020, 23(2):99-101.

[10] Feng J and Han B. Application of Internet of Things Technology in "No. 1 Military Medical Project" HIS [J]. *China Medical Devices*, 2017, 32(9):107-110,114.

[11] Yuan B. The Security Risks and Preventive Measures of the Informatization Construction of Three-level Hospital [J]. *Computer & Telecommunication*, 2018, (Z1):77-78,81.

[12] Yang Y, Wang MY, Luo K, *et al.* Preliminary Study on Internal Control of Hospital Information System Based on Risk Prevention and Control [J]. *Journal of Medical Informatics*, 2020, 41(1):59-62.

[13] Hong HJ and Su XG. Design and Implementation of Server Virtualization in Hospital Information System [J]. *China Medical Devices*, 2017, 32(3):113-116.

[14] Zuang SY, Yang BW and Lin XL. Discussion on Overall Solution of Hospital Informatization Operation and Maintenance [J]. *China Medical Devices*, 2021, 36(1):110-114.

[15] Zheng P, Liu H, Ju WS, *et al.* Investigation and Analysis of the Data Security Status of Hospitals in China [J]. *Journal of Medical Informatics*, 2024, 45(5):71-75.

[16] Zhou WM, Xiang SP, Xiang DC, *et al.* Informatization Construction and Medical Process Optimization of Chest Pain Center Management [J]. *Military Medicine of Joint Logistics*, 2013, 27(7):521-523.