Research on Information Security Management in Hospital Informatization Construction

Zhiying Cao(✉) and Chujun Wu

The Affiliated Changshu Hospital of Soochow University (Changshu No. 1 People's Hospital), Changshu 215500, Jiangsu, China
502921758@qq.com

Abstract. As we enter the information age, a new problem facing hospital information construction is to do a good job in information security protection. General situation of hospital informatization, with the construction and development of hospitals, the degree of informatization is getting higher and higher, and the requirements for information security are also getting higher and higher. Focusing on the quality and service improvement of the hospital, the following measures have been taken in the construction of hospital informatization, and the original software has been upgraded and improved. The information security construction of the hospital is also built around the Equal Security 2.0 standard. The standards and equipment involved in the Equal Security 2.0 are divided into optional items and mandatory items. Combined with the construction of hospital information talents to ensure information security, the information security of the hospital is summarized Construction essentials.

Keywords: Information Security · Information Construction · Smart Hospital

1 Introduction

Without the health of the whole people, there will be no comprehensive well-off society. How to make the broad masses of people enjoy fair, accessible, systematic and continuous health services such as prevention, treatment, rehabilitation and health promotion, medical development in the new era has a long way to go. Informatization has become the driving force of medical empowerment in the new era [1–3]. At the same time, the introduction of a series of national policies will further standardize and promote medical informatization. With entering the information age, a new problem faced by hospital information construction is to do a good job in information security protection. However, with the deepening of hospital informatization construction, although the application of various information software, platforms and systems has brought more convenience to hospital management, its network protection technology has not kept pace with the upgrading of software, platforms and systems, which will bury some hidden dangers in safety. If these software, platforms and systems have security problems, it will impact the whole hospital information management system, and even affect the normal order of the

B. Wang et al. (Eds.): ICMTEL 2023, LNICST 532, pp. 362–369, 2024.
https://doi.org/10.1007/978-3-031-50571-3_26

hospital to a large extent. National Network Security Publicity Week National Network Security and Informatization Work Conference, national network security work should adhere to network security for the people, network security depends on the people, protect personal information security, and safeguard citizens' legitimate rights and interests in cyberspace [4, 5].

2 Research Status

Informatization overview, with the put into use of the Binjiang Hospital and the construction of a medical community, the degree of informatization is getting higher and higher, and the requirements for information security are also getting higher and higher. The current status of the vmware platform: 10 hosts, 4 sets of storage. The status of the hyper-converged platform: 16 hosts, 87T space, all in the telecommunications room, relying on 4 optical fibers to aggregate and connect to the hospital, more than 1,400 computer terminals, and the hospital system has medical information System (HIS), Hospital Big Data Integration Platform, Structured Electronic Medical Record System (EMR), Inspection System (LIS), Nursing Management System (NIS), ECG, Electroencephalogram System (ECG), Medical Image System (PACS), office (OA) system and other basic software. Focusing on the quality and service improvement of the hospital, the following measures have been taken in the construction of hospital informatization, and the original software has been upgraded and improved [6].

(a) Build a patient service platform to improve service quality. The hospital developed the "Changshu No. 1 Hospital" Alipay applet, and at the same time connected to Alipay's "Jiangsu Medical Insurance Cloud applet", which can perform functions such as appointment registration, outpatient settlement, and query of the daily list of hospitalizations [7].
(b) Create and improve the clinical information system to improve the medical level. The upgrade of the integrated system will start in 2022, so that the his system of our hospital can meet the standard of five-level electronic medical records. In the past two years, the medical image system PACS has been continuously upgraded, and the upgraded function has been improved while an advanced 3D reconstruction processing system has been added to facilitate clinical scientific research. At present, the hospital information system is being investigated to lay the foundation for the construction of a smart hospital [8].
(c) Real-time interaction of external data to realize communication without boundaries. There are medical insurance special lines, municipal and regional health information platforms, provincial supervision platforms, telemedicine cloud platforms, and Jiangsu image cloud platforms [9].
(d) Build a hospital big data integration platform to assist management. Realize data cleaning, conversion and fusion of hospital heterogeneous information systems, realize seamless connection of heterogeneous system data, ensure data standardization, standardization and availability in the data center; effectively integrate data from different business systems, quickly and accurately provide reports and propose decision-making basis; integrate hospital-level information application systems, simplify login time, and improve efficiency [10].

3 Information Security Construction

With the development of information construction in smart hospitals and related cloud computing, mobile internet and Internet of Things, the previous security architecture is facing more and more challenges, and various information security accidents occur from time to time in medical institutions. Faced with the severe network security situation, in May 2019, the Basic Requirements for Network Security Level Protection of Information Security Technology (hereinafter referred to as "Equal Security 2.0") was officially released, which brought brand-new security norms and requirements to the medical industry. The information security construction of Hospital is also built around the equal security 2.0 standard [11–13].

3.1 Demand Analysis

Analysis of the review requirements of Equal Security 2.0: Compared with Equal Security 1.0, the new regulations of Equal Security 2.0 have added significant new changes and construction requirements, which are mainly reflected in the following four aspects: Changes of coverage objects. The objects in the new specification not only contain traditional objects, but also add new subjects with the times, such as big data platform, Internet of Things, mobile internet and so on. Changes in safety requirements. The boundary of security expansion is more focused on considering the security risks generated by convenience technologies such as big data technology and Internet technology. Changes of classification structure. Security 2.0 defines two parts: technical part and management part. The technical part focuses on physical environment, communication network, network boundary, computing and overall framework. The management part includes management system, management organization, management personnel, construction tracking and continuous operation and maintenance. Emphasize the security of cloud connection. It not only requires the security of the previous infrastructure and public cloud, but also increases the security content of private clouds such as virtualization, and even involves institutional mandatory audit requirements such as cloud service provider qualification and cloud computing environment [14–16].

Analysis of general information security requirements: physical environment, especially computer room security, including temperature, humidity, static electricity, lightning protection, fire prevention, theft prevention, power supply server, storage and other equipment, needs redundant configuration, equipped with disaster recovery computer room; And terminal security includes dual-link protection, Trojan horse and virus protection, operating system vulnerability patch, hacker attack prevention and network access control; Application data security includes permission setting, password mechanism, authentication, data loss, tampering and disclosure [17–20].

3.2 Safety Scheme and Equipment Selection

In general, the selection of information security scheme and equipment should focus on equal security construction, enhance security awareness, improve security management system, implement network security responsibility and enhance security protection level. Hospital takes HIS as the third-class insurance, LIS as the second-class insurance for

clinical inspection system, PACS as the second-class insurance, portal website as the second-class insurance and Cloud Hospital as the second-class insurance to evaluate the level protection gap. Meet the principle of mandatory construction and optional on-demand construction. See Fig. 1.

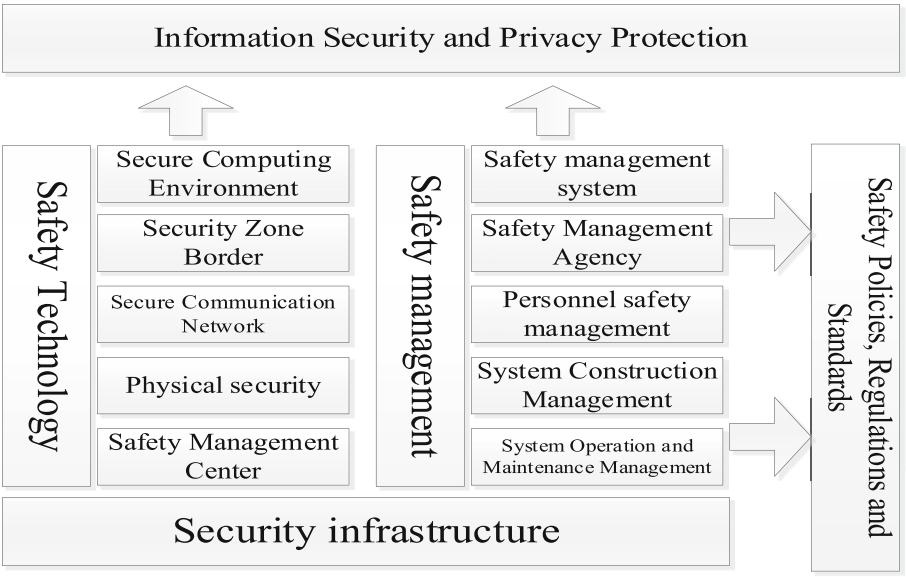

Fig. 1. Information security management architecture

Required for protection requirements:

Firewalls are deployed between different dense networks to realize functions such as area division and access control, and to realize protection between different areas; Intrusion prevention equipment is deployed in the network by serial connection or port mirroring, which is a network security equipment that gives an alarm or takes active response measures when suspicious transmission is found; The gas wall is deployed at the junction of the hospital LAN and the Internet. A network security device for filtering viruses in network transmission. Prevent viruses from invading the intranet from the Internet; The network antivirus software system consists of two parts: control center and terminal. The management end of the system is deployed in the operation and maintenance management area, and the antivirus terminal is deployed in the server or terminal that needs to be protected to perform the final antivirus scanning, intrusion prevention and other security operations. And send corresponding safety data to the safety control center; The audit security system collects logs of all security devices, network devices, host systems and application systems in the network in a unified way, and realizes centralized storage of logs to ensure that they can be retained for more than 6 months; By defining a trusted domain, the access system allows computers in the trusted domain to visit each other, but prohibits computers in the untrusted domain from communicating with computers in the trusted domain, so as to put an end to any form

of illegal access to the network, and thoroughly prevent illegal computers from illegally accessing the network by common and unmanageable ways such as directly inserting network cables, counterfeiting the IP and computer names of legitimate computers in the intranet, directly connecting legitimate computers in the intranet, and private routing. In order to prevent data loss due to human factors or unexpected reasons such as operation errors, system failures, etc., the backup system saves the whole system data or a part of key data in other places through backup; Disaster tolerance system When the computer system suffers from irresistible natural disasters such as fire, flood, earthquake and war, and man-made disasters such as computer crime, computer virus, power failure, network/communication failure, hardware/software error and human operation error, the disaster tolerance system will ensure the security of user data (data tolerance); Audit database obtains traffic through port mirroring, records database activities on the network in real time, conducts compliance management of fine-grained audit on database operations, and gives real-time warning to risk behaviors suffered by the database. By recording, analyzing and reporting the users' access to the database, it helps users to generate compliance reports and trace the source of accidents afterwards. In order to protect the network and data from invasion and destruction from external and internal users, the Fort-Softer uses various technical means to collect and monitor the system status, security events and network activity servers of every component in the network environment in real time, so as to centralize alarm, timely handle and audit responsibility. WAF's vulnerability attack protection can intercept common web vulnerability attacks, such as SQL injection, XSS cross-site, obtaining sensitive information, exploiting open source component vulnerabilities and other common attacks. Internet behavior management is mainly to realize the audit requirements and traffic management of Internet access. Therefore, the external network behavior management equipment will be deployed behind the firewall, and through traffic audit analysis and management, the function of network resource use control will be realized.

Optional security requirements: security situation awareness platform, which senses and discovers the security situation of the whole network from two aspects of logs and network traffic, and provides decision support for hospital information security management in time; Desktop management system can realize the functions of patch management, security configuration and remote desktop assistance of business terminals. The traffic analysis system can fully analyze the utilization rate of network resources, uniformly analyze and process the traffic information collected in a distributed way, and actively detect and collect, analyze and sort out the network resources by using traffic detection, and visually output the interface; Vulnerability scanning is based on vulnerability database, which detects the security vulnerabilities of designated remote or local computer systems by scanning and other means, and finds a kind of security detection behavior that can exploit vulnerabilities. Load balancing realizes real-time monitoring of data centers, links and servers, and rational distribution of data streams, so that all data centers, links and servers can be fully utilized. IT can expand the overall processing capacity of the application system, improve its stability, effectively improve the user's access experience and reduce the IT investment cost; The gateway consists of two independent systems which are connected to the secure and non-secure networks respectively, and the information ferry between the two networks is carried out through

the gateway to ensure that there is no direct physical path between the two systems, so as to achieve the purpose of isolation and exchange; Anti-leakage DLP is deployed in the network to discover and monitor the transmission of sensitive data in network traffic and terminal information data in real time, so as to discover the risk of sensitive data leakage; Data desensitization system protects data by shielding. Provide real-time desensitization of sensitive data driven by roles and permissions; VPN allows foreign employees or operation and maintenance personnel to access intranet resources. After local employees connect to the Internet, they connect to the VPN through the Internet, and then enter the hospital intranet through the VPN. In order to ensure data security, the communication data between VPN server and client are encrypted.

3.3 Planning and Budgeting

Principles of planning and budgeting: meeting the needs of the present and looking forward to the future as a supplement. Combined with the hospital's own information security budget index, consider the upgrade and expansion ability of software and hardware security products and the maintenance period. Considering the difference of security products for different scenes, it involves the differences of virus database. Consider self-maintenance ability, types and requirements of purchased services. Consider the actual number of terminals, real-time concurrent number and reserved amount to determine the number of purchased services.

4 Strengthen the Construction of Talent Team

In view of the talent problem in the field of information security existing in hospital informatization construction at present, hospitals should strengthen the talent team construction in the field of information security to solve this problem. The construction of talents in the field of information security can be mainly carried out from the following two aspects: (1) Intensify the introduction of high-quality professionals in the field of information security. (2) The hospital should strengthen the education and training of the existing information technology and information security personnel, and carry out various forms and rich information technology information security theoretical knowledge and practical skills training through the way of "please come in and go out", so as to continuously improve the technical ability of the existing personnel in the hospital.

5 Summary

We will continue to enhance the awareness of information security, standardize and improve the management systems related to online system, Internet access and open data application. Purchase information security service, legalize software, supplement information security protection measures by relying on experts and third-party resources, and improve information security emergency plan. Strengthen the construction and training of professional talents and improve practical skills. The network security construction will be further strengthened, and the network security work will be carried out according to the requirements of Equal Security 2.0, focusing on the effective application of asset visual management and security situational awareness platform, and realizing the closed-loop control of pre-planning, in-process monitoring and post-tracing.

References

1. Alena, S., Olga, L., Olga, P., Olga, C.: Approaches to information security threats assessment for the official website of the organization. In: USBEREIT 2022, pp. 263–266 (2022)
2. Palko, D., Myrutenko, L., Babenko, T., Bigdan, A.: Model of information security critical incident risk assessment. IN: IEEE International Conference on Problems of Infocommunications Science and Technology, pp. 157–161 (2021)
3. Kabanda, S., Mogoane, S.N.: A conceptual framework for exploring the factors influencing information security policy compliance in emerging economies. In: Sheikh, Y.H., Rai, I.A., Bakar, A.D. (eds.) AFRICOMM 2021, vol. 443, pp. 203–218. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-06374-9_13
4. Nosova, E., Anisimova, L., Murovana, T., Sviatiuk, Y., Iafinovych, O.: Information security system in provision of the economic security and risk management of the enterprise. In: CEUR Workshop Proceedings (PICST 2021), vol. 3188, pp. 21–31 (2021)
5. Stewart, H.: A systematic framework to explore the determinants of information security policy development and outcomes. Inf. Comput. Secur **30**(4), 490–516 (2022)
6. Alimzhanova, Z., Tleubergen, A., Zhunusbayeva, S., Nazarbayev, D.: Comparative analysis of risk assessment during an enterprise information security audit. In: 2022 International Conference on Smart Information Systems and Technologies (SIST), pp. 1–6 (2022)
7. Sizov, V., Kirov, A.: Development of an analytical data processing system for monitoring information security of an informatization object's information support's structure models. In: EEKM 2020, vol. 2919, pp. 218–226 (2021)
8. Alassaf, M., Alkhalifah, A.: Exploring the influence of direct and indirect factors on information security policy compliance: a systematic literature review. IEEE Access **9**, 162687–162705 (2021)
9. Korać, D., Damjanović, B., Simić, D.: A model of digital identity for better information security in e-learning systems. J. Supercomput. **78**(3), 3325–3354 (2022)
10. Yazdanmehr, A., Li, Y., Wang, J.: Does stress reduce violation intention? Insights from eustress and distress processes on employee reaction to information security policies. Eur. J. Inf. Syst. (2022)
11. Brodin, M., Rose, J.: Mobile information security management for small organisation technology upgrades: the policy-driven approach and the evolving implementation approach. Int. J. Mob. Commun. **18**(5), 598–618 (2020)
12. Zhang, X., He, Y.: Information security management based on risk assessment and analysis. In: 2020 7th International Conference on Information Science and Control Engineering (ICISCE), pp. 749–752 (2020)
13. Tariq, M.I., et al. Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks. Sensors **20**(5), 1310 (2020). (36 pp.)
14. Awang, N., et al.: Identification of information security threats using data mining approach in campus network. In: Proceedings of the 24th Pacific Asia Conference on Information Systems: Information Systems (IS) for the Future (PACIS 2020) (2020)
15. Hina, S., Dominic, P., Durai, D.: Information security policies' compliance: a perspective for higher education institutions. J. Comput. Inf. Syst. **60**(3), 201–211 (2020)
16. Wang, Y.: Network information security risk assessment based on artificial intelligence. J. Phys. Conf. Ser. **1648**, 042109 (2020). (8 pp.)
17. Wang, C., Jin, X.: The researches on public service information security in the context of big data. In: ISBDAI 2020, pp. 86–92 (2020)
18. Kang, M., Hovav, A.: Benchmarking methodology for information security policy (BMISP): artifact development and evaluation. Inf. Syst. Front. **22**(1), 221–242 (2020)

19. Alsbou, N., Price, D., Ali, I.: IoT-based smart hospital using cisco packet tracer analysis. In: 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (2022), 6 p.
20. Mezenner, I., Bouyakoub, S., Bouyakoub, F.M.'H.: Towards a Web of Things-based system for a smart hospital. In: IHSH 2020, pp. 22–27 (2021)