2017 3rd International Conference on Social Science and Development (ICSSD 2017)
ISBN: 978-1-60595-517-9

The Security and Privacy Protection of Hospital Information System

Na WANG[1,a] and Jin-guo WANG[2,b,*]

[1]Department of Anesthesiology, The First Hospital of Jilin University, Changchun, Jilin, China

[2]Department of Urology, The First Hospital of Jilin University, Changchun, Jilin, China

[a]wangna080613@163.com, [b]wangjinguolily@163.com

*Corresponding author

Keywords: Security, Privacy, Protection, Hospital, Informationazation

Abstract. The privacy security and defence measures of hospital information system are analyzed, according to the status quo of the development of hospital information system. By investigation of literature, privacy protection system and informationization are introduced and summarized. The suggestions of personal privacy protection are put forward to strengthen hospital information, including strengthening the legislation of privacy protection and cross-border cooperation of multi-organization.

Introduction

Chinese e-commerce has been developing rapidly and has achieved remarkable results, but the services of healthcare and privacy protection have not made great progress. Only by promoting the reform of the relevant system and the establishment of policy, the residents can enjoy the convenient and safe service [1].

The infrastructure construction improves and strengthens popularization of information technology application in our country. Hospital informationization starts with informatization system and legal system construction. Information talent team expands gradually. Informatization has become the significant support of each health management and service work of the hospital [2].

The information construction of hospital in China has been connected with the international standard in the application field of information technology, but the overall level still has a certain gap within the different regions [3].

The Problems Associated with Informationization and Privacy

The Problems Associated with Informationization

Under normal circumstances, the hospital informationization operators are mainly composed of medical personnel and administrative personnel. Most of the operators aren't computer professionals. During the actual operation of hospital information system, there is not a scientific and reasonable operating standard for the correct operation to the information system [4]. Explosion of the network location and Internet virus file exist. Operators often unwittingly use these network systems. They don't use according to the system instruction. Each terminal may cause infections in hospital information system, resulting in the collapse of hospital information system and the loss of data information [5].

Privacy in Hospital

Health information privacy which is also called the patients privacy, mainly refers to the patients in the medical service of the patient's own involved. Due to the need of medical services by medical institutions and medical workers legitimate, disclosure of personal information is illegal. Medical information has very high sensitivity and privacy [6]. There may be a leak and tampering or be illegal

to steal. It will bring great losses to the patients' life, health and property, or even a threat to national security.

Patients' right of privacy is the right of privacy in a specific form of expression. In the process of medical service it is refers to the law. When patients accept the medical service, their personal privacy shall not be leakage and reject illegal infringement of the rights of medical institutions and medical workers [7].

The Countermeasures of Protection

Security Protection Technology

In the defense of hospital information system security, hospital should improve the practical value of the security protection technology, on the basis of the actual effect and characteristics of information system [8]. It improves the safety protection. In the network operations management system, all kinds of antivirus software, the scientific method of access control list is used. The hospital information system security level for multi-level ascension can defense well against various attacks, in the actual operation process [9].

Information management and safety management personnel, on the other hand, still can make scientific use of Internet technology. At the same time it cooperates with DES encryption technology on lots of new information transmission data encryption processing which can be good for all kinds of information data for rapid transfer of science [10].

Hospital security management can fully use of invasive monitoring technology, on the basis of improved quality of information system security monitoring and real-time information system running flow of scientific detection. At the same time, under the influence of software and hardware contact rule analysis technology, the information data depth of all kinds of information is excavated to further improve the completeness and accuracy of information system data [11].

On the basis of information assets identification, in order to meet the demand of information system security as the goal, the design includes the physical security, access control, authorization policy, terminal host protection strategy, the network communication disaster protection policies and strategies which overall moderate and complete method of information security strategy [12].

Privacy Security Monitoring System

In the big data applications of medical service providers, especially very large comprehensive hospital management patients' personal information deals with a lot of sensitive information and plays a vital role in the protection of individual privacy [13].

In view of the demand of personal information privacy protection under the background of medical big data development, it is of great significance to study the application of privacy information protection technology in medical field [14]. The development of information privacy protection technology is based on access control, data encryption, anonymization and other data privacy protection.

Some patients' privacy breaches are due to illegal theft of medical data, while others may be provided or derived by hospital staff or even patients themselves. The office has already warned medicare and medicaid beneficiaries of a common fraud on access to patient insurance information. Healthcare providers should also protect patients' information from education employees [15]. People often call doctors' offices or hospitals, posing as doctors, experts, pharmacies, suppliers, friends, relatives or insurance representatives. Health care providers must teach their employees to identify such calls and provide information only to qualified callers.

Summary

There are the problems that exist in the construction of hospital informationization. In the future in the process of informatization construction, through unified cognition, it attaches great importance to

the management, formulate scientific and long-term development plan and a balanced proportion of capital investment to strengthen the construction of talent team, establish a data exchange platform, strengthen cooperation and communication with suppliers. It will improve the standardization system and ensure the smooth operation of the hospital information construction. It establishes the transaction security requirement for the exchange of certain medical information and manages the information disclosure.

References

[1] Common Criteria for Information Technology Security Evaluation-Part3: Security Assurance Requirements. The International Organization for Standardization. ISO/IEC 15408-3. 1999

[2] Sandhu RS, Coyne EJ, Feinstein HL, et al. Role-based access control models. IEEE Computer. 1996

[3] CIO Results Final Report-2007 HIMSS Leadership Survey. HIMSS. 2007

[4] Information Technology-Coding of Audio-Visual Objects-Part 2: Visual. ISO/IEC 14496-2. 2001

[5] About National Cancer Center. National Cancer Center of Japan. http://www.ncc.go.jp/jp/about/index.html.

[6] Erik Brynjolfsson, Lorin M. Hitt. Computing Productivity: Firm-Level Evidence[J]. Review of Economics and Statistics. 2003 (4)

[7] Hau L. Lee, Kut C. So, Christopher S. Tang. The Value of Information Sharing in a Two-Level Supply Chain[J]. Management Science. 2000 (5)

[8] Gerardine DeSanctis, Marshall Scott Poole. Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory[J]. Organization Science. 1994 (2)

[9] Information technology-Security techniques-Code of practice for information security management. ISO/IEC 17799. 2005

[10] William H. DeLone, Ephraim R. McLean. Information Systems Success: The Quest for the Dependent Variable[J]. Information Systems Research. 1992 (1)

[11] A Respecification and Extension of the DeLone and McLean Model of IS Success[J] . Peter B. Seddon. Information Systems Research. 1997 (3)

[12] Information Technology Infrastructure Library. ITIL. 2001

[13] Kandala S, Sandhu R. Secure Role-Based Workflow Models. proceedings of the 15th IFIP WG 11.3Working Conference on Database Security. 2002

[14] Media Centre. Department of Health UK. http://mediacentre.dh.g ov.uk/.

[15] Control Objectives for Information and related Technology. COBIT. 1996