http://jhmi.sums.ac.ir
J Health Man & Info 2019, 6(4), 133–137

JHMI
Journal of Health Management and Informatics

Original Article

A Survey on Isfahan's Hospital Information Systems Security

Elham Dehghan[1], **Hamid Reza Peikari**[2], **Nahid Tavakoli**[3]*

[1]MSc, Health Information technology, Faculty of Management and Medical Information Sciences, Isfahan University of Medical Sciences, Isfahan, Iran
[2]Assistant Professor, Management, Department of Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran
[3]Assistant Professor, Health Information Technology in Health Research Center, Isfahan University of Medical Sciences, Isfahan, Iran

Abstract

Introduction: The aim of this study is to identify the security status of information on the managerial, technical, and physical dimensions in the information systems of the hospitals affiliated to Isfahan University of Medical Sciences.

Methods: This is an applied descriptive study conducted in 2017-2018. The study population consisted of 35 Information Technology Department Managers (ITDM). The instrument for data collection was adopted and adapted from Mehrayin; this questionnaire consisted of three dimensions, namely managerial, technological, and physical, formatted into a Likert scale. The data were collected by ITDM census sampling and then by mean analysis using SPSS version 22.

Results: From the viewpoint of ITDM, the information security at the hospital information systems was unsatisfactory, with the mean values of 1.37, 1.28, and 1.218 on managerial, technological, and physical dimensions respectively at the hospital information systems.

Conclusion: In order to improve the physical security for this purpose, hospitals need to take measures to physically control the resources, create security policies for areas containing such information as the server room, use physical protection to counter human damages and natural disasters such as power cuts. To improve technological security, it is recommended that technological arrangements should be made to verify the person requesting access to electronic information prior to its application.

Keywords: Security, Hospital Information System, Information Technology.

Article History:
Received: 17 July 2018
Accepted: 8 September 2018

Please cite this paper as:
Dehghan E, Peikari HR, Tavakoli N. A Survey on Isfahan's Hospital Information Systems Security. J Health Man & Info. 2019; 6(4): 133-137.

***Correspondence to:**
Nahid Tavakoli,
Department of Health Information Technology, School of Management and Medical Information Sciences, Salamat Street, Isfahan University of Medical Sciences, Hezar Jarib Alley, Isfahan, Iran
Tel: +98 9133105973
Email: tavakoli@mng.mui.ac.ir
nahid3712@gmail.com

Introduction

The aim of information security management is to protect information and execute proper control standards to eliminate or minimize threats to the organization security (1-3). As the hospital information system is constantly exposed to such perils as theft, change, transformation, and interruptions in providing information, security must receive the greatest attention (4).

Currently, the use of information systems in health care environments provides such potential advantages as improved care, decreased medical errors, increased legibility, and access to information (5). Yet, in recent years, threats to the health information system security have considerably increased. For instance, between the years 2010 and 2013, the report presented by Health Insurance Portability and Accountability Act (HIPAA) is indicative of health information security defects in 29 million patients' cases (6).

According to a survey conducted in USA in 2007, 75% of the patients were concerned about unauthorized disclosure and sharing on websites of their private information (7). In a study, Meidani et al. concluded that the security of Hospital Information Systems (HIS) in the hospitals under study was suffering from a low security condition (8). Of the major reasons for the existing condition, reference can be made to lack of a technical and executive security infrastructure and failure to take effective steps towards protecting the information exchange environment (9). For this reason, issues concerning the security of information have created concerns in the managers of health care centers (10).

Information security has resulted in improved efficacy of the information systems (11). Unfortunately, however, there is no one single procedure thoroughly guaranteeing the security of information. Therefore, there is a need for a set of standards to ensure the best security measures are taken (12). The first step towards programming for hospital information security is to assess the status quo. A multitude of standards have been developed to study the status quo in hospitals. For instance, to create, implement, maintain, and improve the information security system management and security standards, ISO27001 has provided standards, controls, Health Insurance Portability and Accountability Act (HIPAA), and information security programs on three managerial, technological, and physical dimensions to protect the electronic health information, which can be used as a tool to assess the hospital system information security. However, a number of researchers have recommended using a heterogeneous, rather than a homogeneous, standard (10, 13). As the hospital information system, embodying the most personal and most private patient information enforceable over a single network, interconnects all the hospital departments, the security issue is of prime importance to the system (14, 15).

Hence, this study was conducted aiming to assess the information security on three dimensions, namely managerial, physical, and technological, to help take a step towards reinforcing HIS.

Methods

Applied in nature, this study was conducted descriptively in March 2017 and the spring of 2018. The statistical population comprised the functionaries of the IT departments in 35 hospitals affiliated to Isfahan University of Medical Sciences (with the exception of Imam Hossein and Saei Hospitals in Khomini Shahr). For the purpose of this study, as the size of the study population was limited and a census was taken, in order to collect data, Mehrayin questionnaire entitled "Security of the information contained in the information systems of hospitals affiliated to Tehran and Shahid Beheshti Universities of Medical Sciences" was used in 2011. Developed by Mehrayin on the standards of Healthcare Information and Management Systems Society (HIMSS) and Health Insurance Portability and Accountability Act (HIPAA), the questionnaire comprises four sections for the personal details of the participants, focused on the information security in hospital information systems: the managerial, technological, and physical dimensions. Section I comprises six questions on the demography of the study population, including age, gender, education, work experience, employment location, and major. Section II comprises questions on the variables of the study population, including the managerial, technological, and physical dimensions.

The managerial dimension comprises two sections: Policy-making and Training (15 questions). The technological dimension consists of two areas: software and access (18 questions). The physical dimension comprises two areas: Policy-making and Protection (8 questions). The validity of the questionnaire was measured, using both content validity (the views of four professors and specialists in Health Information Management) and face validity (a survey was conducted on a limited number of the statistical population). The reliability of the questionnaire was obtained .77 by using Cronbach's alpha. Hence, the questionnaire is acceptable in terms of both validity and reliability.

In order to run an opinion poll of the participants, the options for each question were scored as: (Yes=1, No=2, Have no idea=0). Upon calculation of the maximum and minimum scores for each section, the distance thus obtained was divided into three score groups. For this study, SPSS version 22 and descriptive statistics were used to analyze the data. To compare the information security status in the hospital information systems at medical care and non-training centers, as well as the opinions of the functionaries of the information technology departments in hospitals on the security of information in hospital information systems, we calculated the mean score for each group.

Results

Most of the participants were males (74.3%) aged 30-50 (51.4%), and held a Bachelor's degree in software engineering (57.1%). A large number of them (42.8%) had 6-10 years' work experience. The findings obtained from three target study areas indicated that the managerial security of HIS had the highest mean (Table 1).

Based on the findings of this study, the mean value for information security on the physical and technological dimensions in the training hospitals was 1.2 with a standard deviation of 0.15 and 1.2 with a SD 0.2, and those for the non-training hospitals were 1.17 with an SD of 0.21, and 1.3 with an SD of 0.26. The information security on the managerial dimension in training and non-training hospitals was 1.44 with an SD of 0.26, and 1.34 with an SD of 0.23 respectively (Table 2).

As the mean value is smaller than the average range of 1.5, the information security is not satisfactory on the managerial, technological, and physical sub-dimensions in the hospital information systems.

Table 1: Information security status on the managerial, technological, and physical dimensions as viewed by the functionaries of the Information Technology Department

Variables	Mean	Standard Deviation
Information Security on Managerial Dimension	1.37	0.55
Information Security on Technological Dimension	1.28	0.50
Information Security on Physical Dimension	1.218	0.36

Table 2: Information security on physical, managerial, and technological sub-dimensions in the hospitals affiliated to Isfahan University of Medical Sciences

Dimensions	Sub-dimensions	Mean	Standard Deviation
Managerial	Policy-making	1.33	0.53
	Training		0.56
Technological	Software	1.28	0.50
	Access	1.27	0.50
Physical	Policy-making	1.32	0.48
	Protective	1.03	0.28

Discussion

Based on the findings of this study, most of functionaries of the information technology departments in the hospitals under the study believed that the hospital information systems were not in a good condition on the managerial, technological, and physical dimensions. The information security in the hospital information systems is an important issue with the major goal of protecting the privacy, security, and safety of the patient (16). Here, the most important results are presented in comparison with other related studies.

Managerial Security

In the views of the functionaries for the information technology departments of the hospitals affiliated to the Isfahan University of Medical Sciences, the present research findings indicate that the information security of the hospital information systems on the managerial dimension is undesirable. Based on a study conducted by Sharifian et al., out of seven cases of obligatory managerial protective mechanisms, only two, i.e. Hazard Management and Data Backup Project, were completely implemented in all the training hospitals of Shiraz University of Medical Sciences (13). Furthermore, according to a study by Meidani et al. conducted during 2014-2015 on four hospitals including Shahid Beheshti, Razi, Koudakan, and Imam Reza, the managerial security was at a low standard; this is consistent with the results of the present study (8). The results of a study by Park et al. indicated that most of the hospitals under the study pursued a documented policy inspected periodically (17). However, the findings of this study indicated that there were no documented standards in the hospitals studied. Therefore, to enhance the function of the protective managerial mechanism, we need to take measures to plan and develop standards, and prepare a documented comprehensive information security policy and inform the employees. Moreover, periodic revision of the standards and policies could improve the security of health information. The results of a study by Mehaeen et al. in 2011 indicated that the hospital information systems affiliated to Tehran University of Medical Sciences and Shahid Beheshti University of Medical Sciences, on the managerial dimension, comprising policy-making and training, became the focus of attention in training and non-training hospitals, receiving high scores; this was not consistent with the results of this study (10),

As for punishment policies, HIPAA holds that an appropriate punishment policy, which is lacking in most hospitals, must be considered for the workforce that has failed to comply with the security policies; this is consistent with a study conducted by Sharifian et al. (13).

As to the undesirable conditions on the managerial dimension, developing a set of policies and documented standards for punishment of violators, training, and users of the information security in the hospital information systems under the study; respect for certain security standards such as documented standards, supervision of workforce; and proportionate punishment for people who have committed breach is indispensable (18).

Technological Security

The findings of this study indicated that in the opinion of the officials in charge of the Information Security Department in the hospitals affiliated to the Isfahan University of Medical Sciences, on the technological dimension, the information security in hospital information systems is undesirable. In a study conducted by Habibifar et al., emphasis was placed on creating a policy supervising the users' access to health information. Furthermore, they observed that every organization needed to have a user ID and a unique password (9). According to a study conducted in Spain in 2015 by Fernandez et al., it was revealed that 62.2% of the information system users used a weak password and 51.7% of them did not use the organizational methods in hospital for proper destruction of confidential information, a fact which is consistent with the results of the present study (19).

Physical Security

As for the information security on the physical dimension, too, the findings revealed that most of the hospitals affiliated to Isfahan University of Medical Sciences were in an undesirable condition. In this context, the results of Canthan's study revealed that a most important threat to the information security in the hospital information system is power cut due to human errors or other technological factors (20). In a study, Mahmoudzadeh and Radrajabi referred to physical security as "the third factor affecting the vulnerability of information systems" (11). In his studies, Trinilanunt listed "power cut" as "the most important threat to hospital information systems" (21). Based on a study conducted by Mehraeen et al., the hospitals (66.6%) affiliated to Tehran University of Medical Sciences as well as all the hospitals (100%) affiliated to Shahid Beheshti University of Medical Sciences had a good score in terms of the information security of the hospital information systems on the physical dimension, which was not consistent with the results of this study. With a mean value of 1.218 in this area, this study revealed a poor performance (7). In view of such existing projects as Sepas, the electronic interconnection of hospitals and creation of HIS in most hospitals, addressing the issue of security as the infrastructure for creation and enjoyment of information technology is of crucial importance. Therefore, this study focused on the information security in hospital information systems (9).

Failure on the part of some hospital employees to help collect the data during the study and restrictions imposed by the security departments of some hospitals for release of the study findings were among the limitations of the study.

Conclusion

In short, the study findings indicated that the target HIS security is at a low level. The weakness in three areas of these systems emphasizes the absence of documented standards and regulations, the presence of user errors due to a variety of reasons, software problems, and inadequate training of users. A highly important point is that lack of written information, firstly, leaves the employees ignorant of their duties for the protection of HIS security; secondly, if employees commit violations, there will be no authority to handle them. Furthermore, despite the fact that in most medical care centers, the use of HIS software has long been started and that considerable efforts have been made in this respect, it seems that there is still an urgent need for identification of the principles and fundamentals of information security and various aspects of its management. Moreover, it is essential that the issue be pursued, especially in the universities of medical sciences vested with the responsibility of maintaining health and medical care across the country. Therefore, this study finds it necessary to enforce laid-down rules, identify the HIS security weaknesses, create the proper ground for the management of the health information technology departments, and take corrective measures about creating rules, policies, and standards as well as train users, and supervise access and other dimensions of the managerial, physical, and technological standards.

Suggestions

It is suggested that training courses such as security training programs should be arranged for users and documented standards and frameworks should be developed and made available to users in order to improve the HIS information security at hospitals.

Acknowledgement

Many thanks go to the School of Medical Management and Communication, Isfahan University of Medical Sciences for their support.

Conflict of Interest: None declared.

References

1. Haufe K, Colomo-Palacios R, Dzombeta S, Brandis K, Stantchev V. Security management standards: a mapping. *Procedia Computer Science*. 2016;100:755-61.
2. Tavakoli N, Ehteshami A, Hassanzadeh A, Amini F. Information Security Management in Isfahan University of Medical Sciences' Academic Hospitals in 2014. *International Journal of Health System and Disaster Management*. 2014;2(3):175.
3. Zarei J, Sadoughi F. Information security

risk management for computerized health information systems in hospitals: a case study of Iran. *Risk Manag Healthc Policy*. 2016;9:75-85. doi: 10.2147/RMHP.S99908.

4. Kahouei M, Abbasi Z. The Prioritization of Effective Factors on Electronic Health Information Security in Medical Centers. *Health Inf Manage*. 2015;12(2):170-82.
5. Farzandipour M, Meidani Z, Gilasi HR, DehghanBanadaki R. Ranking of hospital information systems based on requirements of Iran in 2013. *Journal of Modern Medical Information Sciences*. 2015;1(1):1-9.
6. Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States. *JAMA*. 2015;313(14):1471-3. doi: 10.1001/jama.2015.2252.
7. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*. 2010;6(4):279-314. doi: 10.1504/ijiem.2010.035624 .
8. Meidani Z, Assari MA, Mosavi SG, Ataei-Andezag A. Evaluation of Hospital Information Systems Security. *Health Inf Manage.* 2017;14(5):87-93.
9. Habibifard V, Rabii M, Bahaodini K. Provide a model for the establishment of an information security system in the teaching hospitals of Kerman University of Medical Sciences Based on information security management system. 2011 Oct 19-20. Proceedings of the 1st Congress of IT Application in Health. Sari: Iran; 2011. Persian.
10. Mehraeen E, Ayatollahi H, Ahmadi M. A study of information security in Hospital Information Systems. *Health Inf Manage*. 2014;10(6):779-88.
11. Mahmodzadeh E, Radrajabi M. Security management for information systems. *J Manag Sci*. 2006;1(4):78-112.
12. Susanto12 H, Almunawar MN, Tuan YC. Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*. 2011;11(5):23-9.
13. Sharifian R, Nematollahi M, Monem H, Ebrahimi F. evaluating the security safeguards in hospital information system according to the health insurance portability and accountability act of university hospitals in Shiraz University of Medical Sciences. 2013.
14. Moradyani G, Jahanmeh P, Rasul F. Hospital information systems security by the intrusion detection system. 5th International Conference on Computer Science, Electrical and Electronics Engineering; 2016. Persian.
15. Piri Z, Naser S, Khezri H, Damnabi S. Investigating the functional model EHR security safeguards in the HIS of Tabriz university of medical sciences. *The Journal of Urmia Nursing and Midwifery Faculty*. 2014;12(8):606-12.
16. Masrom M, Rahimly A. Overview of data security issues in hospital information systems. *Pacific Asia Journal of the Association for Information Systems*. 2015;7(4).
17. Park WS, Seo SW, Son SS, Lee MJ, Kim SH, Choi EM, et al. Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. *Healthc Inform Res*. 2010;16(2):89-99. doi: 10.4258/hir.2010.16.2.89.
18. Abbasi R, Bahaadinbeigy K, Zahiriesfahani M, Esmaeili M, Balouchi M, Shokrisanjagi M. Study of the security status of management dimension in hospital information systems of science universities Iranian elected medicine. Proceedings of the 1st Congress of Medical informatics. Mashhad: Iran; 2017. Persian.
19. Fernandez-Aleman JL, Sanchez-Henarejos A, Toval A, Sanchez-Garcia AB, Hernandez-Hernandez I, Fernandez-Luque L. Analysis of health professional security behaviors in a real clinical setting: an empirical study. *Int J Med Inform*. 2015;84(6):454-67. doi: 10.1016/j.ijmedinf.2015.01.010.
20. Samy GN, Ahmad R, Ismail Z. Security threats categories in healthcare information systems. *Health Informatics J*. 2010;16(3):201-9. doi: 10.1177/1460458210377468.
21. Tritilanunt S, Tongsrisomboon A. Risk analysis and security management of IT information in hospital. *International Journal of Computer and Information Technology*. 2014;4(2).