Health Information Security in Hospitals: the Application of Security Safeguards

Esmaeil Mehraeen[1], Haleh Ayatollahi[2], Maryam Ahmadi[2]

[1]Department of Health Information Management, School of Paramedicine, Tehran University of Medical Sciences, Tehran, Iran
[2]School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran

Corresponding author: Haleh Ayatollahi.
E-mail: ayatollahi.h@iums.ac.ir

doi: 10.5455/aim.2016.24.47-50
ACTA INFORM MED. 2016 FEB; 24(1): 47-50
Received: 18 November 2015 • Accepted: 05 January 2016

ABSTRACT

Introduction: A hospital information system has potentials to improve the accessibility of clinical information and the quality of health care. However, the use of this system has resulted in new challenges, such as concerns over health information security. This paper aims to assess the status of information security in terms of administrative, technical and physical safeguards in the university hospitals. **Methods:** This was a survey study in which the participants were information technology (IT) managers (n=36) who worked in the hospitals affiliated to the top ranked medical universities (university A and university B). Data were collected using a questionnaire. The content validity of the questionnaire was examined by the experts and the reliability of the questionnaire was determined using Cronbach's coefficient alpha (α=0.75). **Results:** The results showed that the administrative safeguards were arranged at a medium level. In terms of the technical safeguards and the physical safeguards, the IT managers rated them at a strong level. **Conclusion:** According to the results, among three types of security safeguards, the administrative safeguards were assessed at the medium level. To improve it, developing security policies, implementing access control models and training users are recommended.

Key words: Information security, Hospital information system, Health information technology, security, safeguard.

1. INTRODUCTION

Currently, healthcare organizations not only provide healthcare services, but also try to compete with each other to earn high scores on audits and accreditations. One of the approaches found helpful to improve the quality of health care is the use of information technology and information systems. The hospital information system is the most widely used system in hospitals to complete daily tasks and to facilitate communication between different departments inside and outside the organization. (1)

Generally, the use of hospital information systems has many advantages for healthcare providers and patients. This system has potentials to increase the accessibility of clinical information and to improve clinical and public health research. However, the use of this system has resulted in new challenges, such as concerns over health information security. Issues, such as maintaining confidentiality and preventing unauthorized access to clinical data are among main concerns that need adequate attention during all stages of data entry, storage, use, and transfer (1, 2). In fact, the issue of health information security is much more complicated than what expected. On one hand, patient information is highly sensitive and need to be kept secure and confidential, on the other hand different healthcare providers may need to get access to them (3, 4). Moreover, the security of heath information is not a local issue, and needs to be considered at a macro level to comply with national regulations and standards. In this case, different hospitals would be able to follow a standard guideline to improve information security in their settings (5, 6). It is notable that security practices include management processes for detecting and mitigating information risks as well as implementing technical safeguards. However, many healthcare organizations consider information security as a technical issue. This view has to be changed to a more holistic socio-technical perspective on information security and has to empha-

Answer Question	YES (%)	NO (%)
Have all workstations and computers been verified?	26 (89.7%)	3 (10.3%)
Is there any preparation plan for preventing problems in information flow?	22 (75.9%)	7 (24.1%)
Have the risks of natural hazards been anticipated?	13 (44.8%)	16 (55.2%)
Is there any preparation plan for preventing physical damage to the systems?	27 (93.1%)	2 (6.9%)
Is the hardware repaired by the professionals?	27 (93.1%)	2 (6.9%)
Is the software repaired by the professionals?	28 (96.6%)	1 (3.4%)
Is there any access control for a server room?	23 (79.3%)	6 (20.7%)
Have the computer equipment been insured?	1 (3.4%)	28 (96.6%)
Are computers checked periodically?	27 (93.1%)	2 (6.9%)
Is there any physical protection for the equipment and the server?	16 (55.2%)	13 (44.8%)

Table 1. The status of physical safeguards used in the university hospitals

size the importance of integrating technical solutions with organizational security culture, policies, and education (7).

It is expected that the employees of healthcare organizations to be trained on the principles of information security and data protection. Otherwise, a lack of training, a lack of instructions for managing security issues, and a lack of clear and documented policies to deal with the risk factors may raise problems for the employees and organizations (5, 6). To investigate information security in hospitals, three main safeguards namely administrative, technical, and physical safeguard should be taken into account (3). According to the literature review, although a number of studies have been conducted about the information security in hospital information systems, most of these studies have only focused on one of the safeguards noted above (8, 9). This paper aims to assess the status of information security in terms of administrative, technical and physical safeguards in the university hospitals.

2. METHODS

This was a survey study in which the participants were information technology (IT) managers (n=36) who worked in the hospitals affiliated to the top ranked medical universities (university A and university B). It is notable that in the present study, the Hospital information system was not the same in all hospitals and seven HIS companies provided the university hospitals with different software. Due to the limited number of participants, no sampling method was used. Data were collected using a questionnaire which was designed based on the criteria and standards suggested by Healthcare Information and Management Systems Society (HIMSS) (10), Health Insurance Portability and Accountability Act (HIPAA) (11) and reviewing the relevant literature (12-15).

The questionnaire included four sections: demographic characteristics of the participants (6 questions) and questions related to the administrative (29 questions), technical (27 questions) and physical safeguards (15 questions). The answers to the questions were scored as follows (Yes=2, No=1, and Do not know=0). In terms of the content validity, the questionnaire was examined by four experts in the field. The reliability of the questionnaire was determined using Cronbach's coefficient alpha (α=0.75).

3. RESULTS

In this study, 29 IT managers (80.5%) answered the questionnaire. About half of the participants were men (51.4%) and their age range was (25-30) years old (51.4%). Most of them had an academic degree (B.Sc.) in computer science (74.2%) and the work experience of (1-10) years had the highest frequency (77.1%).

The second part of the questionnaire was related to the administrative safeguards. This section was divided in two subsections, namely; policy making and training. The IT managers agreed that the institutional data access policy might be changed overtime (n=28, 96.6%). However, there was no specific policy regarding patients' access to their information (n=23, 79.3%) or sanction over unauthorized access to the information (n=20, 69%). In terms of training, all of the IT managers believed that users knew how to keep a username and a password securely (n=29, 100%). In the administrative section of the questionnaire, the minimum score was zero and the maximum score was 58. The score range was divided into three categories (0-18), (19-38) and (39-58) to be able to interpret the results as a weak, medium or strong level of security. The results showed that the score of this section for about half of the hospitals affiliated to university A (52.3%) and university B (50%) was between 19 and 38 which implied a medium level for administrative safeguards.

The third part of the questionnaire was related to the technical safeguards. This section was divided into three subsections, namely; software security, password protection and access control. The IT managers believed that to improve the security of the system, antivirus software were used (n=28, 96.6%) and servers were examined and tested particularly after repairing (n=28, 96.6%). In terms of password protection, IT managers agreed that each of the users had a unique password (n=28, 96.6%); however, most of the time, there was no expiry date for the passwords (n=16, 55.2%). Concerning access control, most of the IT managers (n=28, 96.6%) noted that it was easy for the IT staff to recognize the identity of the users. However, there was no time limit for using the system by the users (n=27, 93.1%). In total, the minimum score was zero and the maximum score was 54 for this section. The score range was divided into three categories of weak (0-17), medium (18-36) and strong (37-54). According to the IT managers' perspectives, in terms of the technical safeguards of information security, most of the hospitals affiliated to university A (75%) were scored between 37 and 54 which showed a strong level of technical security. In university B, the score of this section for most of the hospitals (50%) was between 18 and 36 indicating a medium level of technical security. Overall, the highest frequency of the IT managers (51.7%) believed that the technical safeguards were strong.

The physical safeguards were the third section of the questionnaire (Table 1). This section included two subsections, policy making and physical protection. Regarding policy making, most of the IT managers (n=25, 86.2%) believed that there were institutional policies concerning physical security of computer equipment, and even repairing these systems (n=21, 72.4%). In terms of the physical protection, most of the IT managers (n=27, 93.1%) noted that the software and hardware repair was undertaken by the professional staff. However, the physical equipment was not insured (n=28, 96.6%). For this section, the minimum score was zero and the maximum score was 30. The score range was divided into three categories of weak (0-9), medium (10-20) and strong (21-30). The findings showed that most of the hospitals affiliated to university A (66.6%) and all of the hospitals affiliated to university B (100%) were scored between 21 and 30 which showed a strong level of physical security.

4. DISCUSSION

As hospitals collect, use, and store personal and clinical information, the risks of information leakage and breaching privacy and security in their settings are more serious than any other organizations. Therefore, they should pay more attention to the security issues according to the rules, regulations and medical laws (16, 17).

In the current study, the status of three safeguards of information security was investigated in 29 university hospitals. According to Park et al, among three safeguards of information security; namely, administrative, technical and physical safeguard, the administrative safeguard is the most vulnerable one (18). The results of the current study showed that overall; the administrative safeguards were arranged at a medium level. The IT managers agreed that the there was no specific policy regarding patients' access to their information and punishing unauthorized access to the information. Therefore, in terms of the administrative procedures, hospitals are recommended to be equipped with detailed policy documents. Moreover, all staff, especially new employees should be trained on their responsibilities for protecting information. Not only effective security strategy is required inside the hospital, but also security requirements should be suggested in third party agreements (16). Other studies indicate that access level, monitoring the accuracy and completeness of information and implementation of educational programs for increasing users` knowledge about issues related to information security are the main components of the administrative safeguard and are of high importance (19).

In terms of the technical safeguard, the results showed that the IT managers rated the technical safeguard at a strong level. However, it might be overestimated. There were examples of weaknesses in the technical safeguards. For example, in terms of password protection, the IT managers agreed that each of the users had a unique password; however, there was no formal procedure for issuing or destroying passwords.

According to Win, although password checking is included in hospital information systems, it does not ensure the security of the systems. Thus, in addition to the password, there should be some mechanisms to enhance information security (20). Similarly, Collmann et al stated that to protect sensitive health information, health care organizations should build safe organizational contexts and follow appropriate information security practice and regulations (21). Concerning technical solutions, hospitals are recommended to set security policies and procedures for exchanging information. The access of unauthorized staff to medical information should be protected to ensure the security of the information systems. Obviously, with respect to the technology advancement, the scope and the level of technical vulnerability needs to be determined and reviewed regularly (16).

Concerning physical safeguards, the results showed that most of the hospitals were rated at a strong level. In this regard, the results of Ganthan's study showed that the physical safeguards in healthcare organizations has an important role in improving overall information security and can be one of the most important threats for information security (22). Hospitals are recommended to improve the physical and environmental security by defining secure areas and applying physical entry controls for the security of information assets. The disposal and re-use of related equipment should be defined as well (15).

5. LIMITATIONS

In this study, the status of information security in the university hospitals was assessed based on the IT managers' perspectives. As a result, self-reported data were used to report the findings. The IT managers might overestimate the status of information security in their hospitals. However, the hospitals were different in terms of organizational, technical and physical characteristics. Therefore, the researchers believed that the results might not be affected by self-reported data.

6. CONCLUSIONS

A number of methods exist to ensure the security and privacy of health information. This study focused on assessing the status of information security in the university hospitals with respect to three main safeguards, namely administrative, technical and physical. As the administrative safeguards were assessed at the medium level, developing security policies, implementing access control polices, training users, providing appropriate authorization and supervision of workforce members, and applying appropriate sanctions against unauthorized access to information are recommended.

- Author's contribution: author and all co-authors of this paper have contributed in all phases if it's preparing. Final proof reading was made by first author.
- Acknowledgments: This study was funded and supported by Tehran University of Medical Sciences (TUMS); Grant no. 449.
- Conflict of interest: The authors declare that they have no conflict of interest.

REFERENCES

1. Deshmukh P, Croasdell D. HIPAA: Privacy and security in health care networks. In: Tan J. (editor). Medical informatics: Concepts, methodologies, tools, and applications. New York: IGI Global, 2009: 1897-99.
2. Cavalli E, Mattasoglio A, Pinciroli F, Spaggiari P. Information security concepts and practices: the case of a provincial multi-specialty hospital. Int J Med Inform. 2004; 73(3): 297-303.

3. Ray A, Newell S. Exploring information security risks in healthcare systems. In: Rodrigues J. (editor). Health information systems: Concepts, methodologies, tools, and applications. New York: IGI Global, 2010: 1716-8.
4. Fernando J. Factors that have contributed to a lack of integration in health information system security. J Inform Techn Healthcare. 2004; 2(5): 313-28.
5. Misic J, Misic V. Implementation of security policy for clinical information systems over wireless sensor networks. Ad Hoc Networks. 2007; 5(1): 134-44.
6. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security requirements and solutions in electronic health records: lessons learned from a comparative study. J Med Sys. 2010; 34(4): 629-42.
7. Kwon J, Johnson ME. Security practices and regulatory compliance in the healthcare industry. J Am Med Inform Assoc. 2013; 20: 44–51.
8. Pourasghar F. The role of information technology on documentation and security of medical data [PhD Thesis]. Sweden: Department of learning, information, management and ethics Karolinska Institutet, Stockolm, 2009.
9. Fernández-Alemán, Carrión Señor I, Lozoya PAO, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform. 2013; 46: 541-62.
10. Healthcare Information and Management Systems Society (HIMSS). Introduction to the toolkit & security risk assessment basics. [Online] 2015 [Cited 2015 June 11]. Available from: http://www.himss.org/resourcelibrary/TopicList.aspx?MetaDataID=1814
11. Department of Health & Human Services. [Online] 2015 [Cited 2015 March 26]. Available from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.
12. Kemp L. Information security management: An entangled research challenge. Inform Sec Tech Rept. 2009; 14(4): 181-4.
13. Lusignan S, Chanb T, Theadoma A, Dhoula N. The roles of policy and professionalism in the protection of processed clinical data: A literature review. Int J Med Inform. 2007; 76(4): 261-68.
14. Coleman J. Assessing information security risk in healthcare organizations of different scale. Int Cong Ses. 2005; 1268: 125-30.
15. Cazier J, Medlin B. How secure is your information system? An investigation into actual healthcare worker password practices. Perspectives in Health Inform Manage. 2006; 3(8): 1-7.
16. Park WS, Seo SW, Son SS, Lee MJ, Kim SH, Choi EM. Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. Healthc Inform Res. 2010 June;16(2): 89-99.
17. Ness R. Influence of the HIPAA privacy rule on health research. J Am Med Assn. 2007; 298(18): 2164-70.
18. Park W, 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.
19. Behnam S. Comparative study of levels of access and confidentiality of medical records in selected countries with Iran [Thesis in Persian]. Iran University of Medical Sciences and Health Services, Faculty of Management and Information, 2004.
20. Win KT. A review of security of electronic health records. HIM J. 2005; 34(1): 13-8.
21. Collmann J, Cooper T. Breaching the security of the Kaiser Permanente internet patient portal: the organizational foundations of information security. J American Med Inform Assoc. 2007; 14(2): 239-43.
22. Ganthan S, Rabiah A. Security threats categories in healthcare information systems. Health Informatics J. 2010; 16(3): 201-9.