Risk Management and Healthcare Policy

Dovepress
open access to scientific and medical research

Open Access Full Text Article

ORIGINAL RESEARCH

Information security risk management for computerized health information systems in hospitals: a case study of Iran

This article was published in the following Dove Press journal:
Risk Management and Healthcare Policy
27 May 2016
Number of times this article has been viewed

Javad Zarei[1]
Farahnaz Sadoughi[2]

[1]Health Information Management, Health Management and Economics Research Center, School of Health Management and Information Science, Iran University of Medical Sciences, Tehran, Islamic Republic of Iran, [2]Health Information Management Department, School of Health Management and Information Science, Iran University of Medical Sciences, Tehran, Islamic Republic of Iran

Background: In recent years, hospitals in Iran – similar to those in other countries – have experienced growing use of computerized health information systems (CHISs), which play a significant role in the operations of hospitals. But, the major challenge of CHIS use is information security. This study attempts to evaluate CHIS information security risk management at hospitals of Iran.

Materials and methods: This applied study is a descriptive and cross-sectional research that has been conducted in 2015. The data were collected from 551 hospitals of Iran. Based on literature review, experts' opinion, and observations at five hospitals, our intensive questionnaire was designed to assess security risk management for CHISs at the concerned hospitals, which was then sent to all hospitals in Iran by the Ministry of Health.

Results: Sixty-nine percent of the studied hospitals pursue information security policies and procedures in conformity with Iran Hospitals Accreditation Standards. At some hospitals, risk identification, risk evaluation, and risk estimation, as well as risk treatment, are unstructured without any specified approach or methodology. There is no significant structured approach to risk management at the studied hospitals.

Conclusion: Information security risk management is not followed by Iran's hospitals and their information security policies. This problem can cause a large number of challenges for their CHIS security in future. Therefore, Iran's Ministry of Health should develop practical policies to improve information security risk management in the hospitals of Iran.

Keywords: information security, risk management, health information systems, hospital

Background

In recent years, rapid growth of information and communication technologies and increasing pressures for reducing health care costs, improving health care quality, ensuring patient safety, and reducing medical mistakes have led to increasing use of computerized health information systems (CHISs) in health care organizations.[1–3] Currently, use of CHIS is a basic requirement for any health care organization such as hospitals.[4] CHIS refers to any computer system capturing, storing, managing, and transmitting personal or organizational health information in health care sectors.[5] One of the major challenges of CHIS use is information security.[6–8] Patients' personal health information contained in the CHIS is considered the most confidential personal information that should be protected.[9] Electronic health information recording increases the risk of unauthorized access and disclosure of information. In case of unauthorized disclosure of information, patients, practitioners, and hospitals run into serious problems.[10]

Correspondence: Farahnaz Sadoughi
Department of Health Information Management, School of Health Management and Information Sciences, Iran University of Medical Sciences, No 6, Rashidi Yasemi Street, Vali-e Asr Avenue, Tehran 1995614111, Islamic Republic of Iran
Tel +98 21 8879 4302
Fax +98 21 8888 3334
Email Sadoughi.f@iums.ac.ir

Computerized information systems of organizations are faced with a variety of internal and external threats, which can cause different types of damages.[11] They can have adverse effects on organizational operations, information assets, individuals, organizations, and national areas of studies.[12] Therefore, information security is crucial for organizational survival, minimization of threats endangering organizational operations, and protection of confidentiality, integrity, and availability of information.[13,14] The main objective of "information security" is implementing appropriate control measures for eliminating or minimizing the impacts of different organizational security-related threats and organizational vulnerabilities.[15] The main question is how information security can be effectively and economically implemented in organizations. The answer is Information Security Risk Management (ISRM).[16]

ISRM is a structured and continuous process with the purpose of identifying, evaluating, and minimizing some types of risks, as well as achieving appropriate acceptability.[17] ISRM is very important for organizational successful information security programs for the following reasons.[18] First, information security risks are not constant over time and vary depending on the conditions of the organizations, development and changes in the information system, new users, and so on.[19] ISRM is one of the ways to reduce the negative impact of risks on the organization.[20] Second, through risk management, organizations can concentrate on resources of high-risk areas and can manage them by using appropriate and measurable ways while limiting risks reasonably.[21] Third, one of the characteristics of a successful security program is cost–benefit analysis of the implementation of information security controls. This accurate analysis is performed by the risk management process.[16,19]

In Iran, a hospital is the main health care organization.[22] Thus, one of the major pieces of health information is recorded at hospitals. In the past decade, CHIS has been increasingly used by Iran's hospitals. Accordingly, clinical, financial, and administrative activities of hospitals are increasingly dependent on the performance of the CHIS, as compared with the past.[23] Therefore, ensuring information security in these systems is of crucial importance for the hospitals. However, in recent years, CHIS security at Iran's hospitals has faced greater challenges. In 2014, for the purpose of reducing public costs of health care, a health reform plan was implemented as one of the major policies of the new government.[24] Accordingly, hospitals are required to connect their hospital information system programs to the Iranian system of electronic health records (SEPAS system) through the Internet. Connection through public Internet network considerably increases the risks of unauthorized access to information; meanwhile, some findings reveal lack of specified rules on confidentiality of patient information in electronic health systems of hospitals.[25] Moreover, in recent years, due to the disputes concerning Iran's nuclear program and Iran's disagreements with Western countries and some of the Middle East countries, Iran's computer information system has been exposed to cyber threats, such as the Internet viruses Stuxnet and Flame.[26–28] These viruses, according to many information security experts in the world, are very complex and cannot easily be confronted.[27,29] In 2014, the information security firms Kaspersky Lab and Symantec reported an advanced espionage malware (Regin), one of whose target countries was Iran.[30,31]

Considering the information security risks at Iran's hospitals and importance of ISRM in reducing and minimizing adverse effects of information security risks, as well as the effectiveness of the information security programs in hospitals, this study investigates the ISRM status at hospitals of Iran. Findings of this study can provide a comprehensive view of the ISRM situation and its place in health information security policies of hospitals and can help researchers and policy makers interested in ISRM in health care.

Materials and methods

This applied research is a descriptive cross-sectional study conducted in 2015. All active hospitals in Iran (until August 2014) were studied. In the first step, the research instrument for the assessment of ISRM situation in the hospitals of Iran was designed. To design the instrument, key processes of ISRM were identified by using the literature review in related information sources. The gathered data included guidelines, frameworks, standards, and methodologies for information security risk assessment and risk management, previous studies on ISRM in the hospitals, and other documents related to ISRM.

Several search engines and databases such as Google Scholar, Institute of Electrical and Electronics Engineers Digital Library, Association for Computing Machinery Digital Library, and PubMed were searched to find the relevant documents. Documents were identified by the following keywords: "Information security risk management" and "Information security risk assessment", combined with the terms "Standard", "Method", "Model", "Framework", "Guideline", and "Best practice" or "Hospital", and "Health" in English language. We confined our search to documents published from 2000 to 2014. Inclusion criteria for selecting resources included the

following: 1) availability of documents in English language and 2) free access to full-text documents. Non-full-text articles and documents were excluded. Literature was reviewed to data saturation level. When at least a risk assessment and management process principle appears in five retrieved sources, including articles, books, standards, guidelines, and methodologies, it was considered data saturation level. The data saturation level was determined based on three experts' judgment (specialist in information security risk management). Sampling was not performed, and all the relevant literature, retrieved based on inclusion criteria, were evaluated.

A checklist was used to extract content from retrieved documents. In total, the specific guidelines, standards, and methodologies for information security risk assessment and risk management were as follows: International Standard Organization/International Electrotechnical Commission (ISO/IEC) 27005,[32] National Institute of Standards and Technology Special Publication 800-30 (NIST SP 800-30),[12] Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) allegro,[33] Method for Harmonized Analysis of Risk (MEHARI),[34,35] Metodologia de Analisis y Gestion de Riesgos de los Sistemas de Informacion (MAGRIT),[36] information technology (IT)-Grundschutz,[37] Information Technology Security Guidance- IT security risk management: a lifecycle approach-33 (ITSG-33),[38] Security Officers Management & Analysis Project (SOMAP),[39] Threat Agent Risk Assessment (TARA),[40] CORAS,[41] Threat Vulnerability and Risk Analysis (TVRA),[42] Factor Analysis of Information Risk (FAIR) Analysis (O-RA),[43] and Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)[44]; and international standards of information security management (ISM), including ISO/IEC 17799[45] and ISO 27799,[46] were identified and surveyed. Moreover, eight studies related to information security risk assessment and risk management in hospital,[47–54] one report,[55] and one book[56] were retrieved and reviewed. In the second step, key processes of ISRM were extracted from the retrieved literatures. Figure 1 shows these stages.

In the third step, based on results of the previous stage, health information management and computer experts' opinions, and observations of the five selected hospitals, a comprehensive form was designed to assess the status of ISRM for computerized health information systems, including four distinct parts encompassing general information about hospitals, specifications of computerized health information systems, information security incidences, and self-assessment checklist of ISRM. Its content validity was confirmed by 12 experts of health information management, medical informatics, information technology (IT), and computer engineering (three professionals per area of study).These scholars were selected on the basis of their previous work experience in the hospital's IT departments or their familiarity with the structure of the IT department in the hospitals of Iran. For data collection, this questionnaire and its guideline were sent to all 908 active hospitals in Iran by the Ministry of Health of Iran. To remove any possible ambiguity, an instruction sheet was attached to this questionnaire, explaining all sections. The hospitals were selected with regard to their CHIS application, such as hospital information system, Electronic Medical Record, Patient's Admission and Discharge Systems, and so on. Hospitals that did not use CHIS at the time of this research were excluded. To facilitate and expedite the collection of data, this form was placed electronically in the official Web site (portal) of the Ministry of Health of Iran and hospitals were asked to register the relevant information in the aforementioned Web site.

After data collection, primary analysis was conducted in order to fix the defects and correct the information. Then,

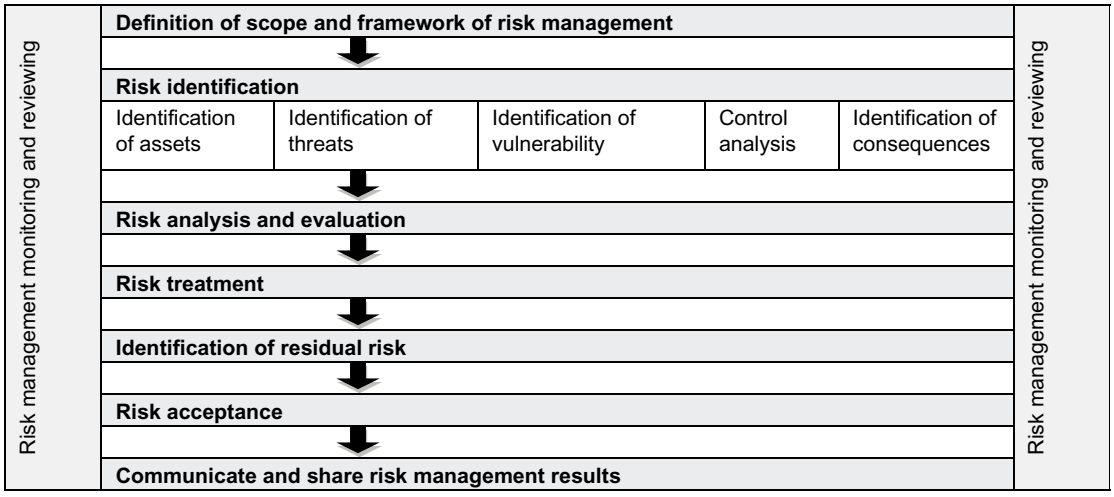

Figure 1 Key process of information security risk management.

hospitals were asked through a second formal letter to take action to correct the defect. The collected data were analyzed by using descriptive statistics (frequency) in Excel 2003 software.

Ethical issues

The study was approved by the Deputy of Research and Technology of the Iran University of Medical Sciences, Tehran, Iran.

Results

Information related to the studied hospitals

Out of 908 active hospitals in Iran, 551 hospitals (60.7%) participated in the study. Two hospitals were setting up CHIS at the time of this research. Therefore, they were excluded from the study and 549 hospitals (60.5%) were studied. The highest percentage of participation in the study was related to the hospitals affiliated to the Medical Sciences Universities (Table 1).

IT personnel in the studied hospitals

Most of the hospitals (540 instances, 98.5%) had IT personnel. Conversely, they had Chief Information Security Officers (CISOs). On average, one IT personnel existed per 77 computer systems and also per 84 bed counts in the hospital.

Information security policies and procedures in hospitals

There were some policies and procedures for information security in 379 hospitals (69%). Only in eight hospitals (1.4%), these policies and procedures were provided based on specific information security standards such as ISO/IEC 27001. Additionally, all of these hospitals had a framework for ISM. Other hospitals pursued Iranian Hospitals Accreditation Standards. Only eight hospitals had a framework for ISRM, of which seven hospitals implemented security policies and procedures of specific information security standards. None of the hospitals had a systematic approach for ISRM (Table 2).

Table 1 Distribution of hospitals in Iran that participated in the study

Type of ownership	Active hospitals in Iran			Hospitals participating in the study			Participation percentage
	Teaching hospital	Nonteaching hospital	Total	Teaching hospital	Nonteaching hospital	Total	
Universities of Medical Sciences	241	324	565	184	220	404	72.2
Private	2	140	142	1	66	67	46.5
Military	6	45	51	2	6	8	15.7
Charity	1	29	30	0	12	12	40.0
Others	20	100	120	9	49	58	48.3
Total	270	638	908	196	353	549	60.5

Table 2 Policies and procedures for information security in hospitals

Type of ownership	Policies and procedures for information security		Framework for information security management		Framework for information security RA/RM		Number of hospitals
	Based on Iranian Hospital Accreditation Standard	Policy and procedures based on information security standards	Defining framework for ISM	Using a systematic approach to defining framework for ISM	Defining framework for information security RA/RM	Using a systematic approach to defining framework for information security RA/RM	
	Frequency	Frequency	Frequency	Frequency	Frequency	Frequency	
Universities of Medical Sciences	245	3	4	2 Missing: 2	3	0 Missing: 1	404
Private	65	2	3	0	3	0	67
Military	4	1	1 Missing: 1	0 Missing: 1	1 Missing: 1	0 Missing: 1	8
Charity	11	0	0	0	0	0	12
Other organizations	54	2	2	1	1	0	58
Total	379	8	10 Missing: 1	3 Missing: 3	8 Missing: 1	0 Missing: 2	549

Abbreviations: ISM, information security management; RA/RM, risk assessment/risk management.

Process of information security risk identification at hospitals

Among the main activities of information security risk identification, only identification of assets, identification of threats, and control analysis were performed systematically in a few hospitals; these hospitals took ISM into consideration. At some hospitals, there was no sequence among the subactivities related to information security risk identification, ie, the activities were performed unrelated to their previous and subsequent activities. Altogether, the obtained findings indicated the lack of a systematic approach for risk identification. Among the subactivities related to information security risk identification, the highest frequency was related to information assets identification (415 instances; Table 3).

Process of information security risk analysis and evaluation at hospitals

None of the subactivities related to the process of information security risk analysis and evaluation was performed systematically at the selected hospitals. Although risk evaluation was not carried out in hospitals, 124 hospitals attempted to prioritize the information security risks (Table 4).

Processes of information security risk treatment and risk acceptance at hospitals

No comprehensive plan was conducted for reducing information security risks. The main approach of hospitals to risk treatment was risk reduction, along with implementation of basic information security safeguards. None of the subactivities related to the processes of information security risk treatment and acceptance in hospitals was performed systematically (Table 5).

Residual risk acceptance and mitigation occurred only in six hospitals, which established ISM policies and procedures based on specific information security standards.

Communicating and sharing risk management results at hospitals

Communicating and sharing of risk management results were not observed in any of the hospitals.

ISRM monitoring and reviewing at hospitals

Information security policies and procedures, as well as implementation of control measures, were continuously monitored and reviewed at 146 hospitals and 142 hospitals, respectively, though it was not done systematically (Table 6).

Discussion

The results show lack of a systematic and comprehensive approach to ISRM at the studied hospitals. Although some activities are conducted for risk identification, risk evaluation, and risk treatment, they are not systematically structured, ie, the hospitals do not use the specialized methodologies or standards for ISRM. Therefore, there is no coherence between the activities related to ISRM at most hospitals. ISRM is a systematic, structured, and continuous process, through which various interdependent steps are taken, and the activities of each step are affected by the results of the previous stage.[55] Without following a systematic and structured method, accurate risk assessment and management is not possible. Hence, various standards, methodologies, and tools are developed all over the world by public and private organizations, agencies, and different companies for information security risk assessment and management.[55–57]

Only a small number of hospitals pursue ISRM framework; yet, they are not systematically structured. Defining a framework for risk management is one of the initial steps of implementation of the ISRM process.[55] The framework development specifies scopes of risk management activity, required resources, key stakeholders, and limitations and boundaries of the risk management process and also makes a contribution to the ISRM process.[32] Lack of risk management framework at Iran's hospitals indicates weakness of information security policies and procedures. Information security policies are developed in conformity with Iranian Hospitals Accreditation Standards. Accordingly, hospitals are obliged to formulate policies and procedures for key processes in each department.[58] But these standards are very limited, vague, and incomplete, as compared with specific standards, rules, or guidelines for information security, and do not cover many of the important details and processes of information security.

Only in a small number of hospitals, this policy was formulated based on special standards of information security, such as ISO/IEC 27001. All these hospitals had a framework for ISRM. Information security standards such as the ISO 2700X series provide an appropriate framework for organizational ISM.[59] Using standard methods for ISM and ISRM is of great importance. Although Iran is a member of the ISO and ISO 2700X standards have been accepted as the national standards of Iran, hospitals do not use these standards due to the lack of specific national laws

Table 3 Information security risk identification in hospitals

Type of ownership	Asset identification			Threat identification			Vulnerability identification	
	Identification of assets	Evaluation and prioritization of assets	Using systematic approach to asset identification	Identification of threats: sources	Identification of threats: events	Using systematic approach to threat identification	Identification of vulnerability	Using systematic approach to vulnerability identification
	Frequency	Frequency	Frequency	Frequency	Frequency	Frequency	Frequency	Frequency
Universities of Medical Sciences	294	140 Missing: 2	2 Missing: 1	198	186	2 Missing: 1	101	0
Private	55	26	2	38	25	2	21	0
Military	7	5	1	5	3	0	4	0
Charity	9	5	0	7	3	0	2	0
Other organizations	50	18	2	32	27	2	21	0
Total	415	194 Missing: 2	7	280	244	6 Missing: 1	149	0

on health information security. One of the reasons for this problem is weakness of major policies and rules associated with the health information security of Iran. Some studies reveal that rules of health information in Iran have some defects.[60] In many developed countries such as Australia[61] and the US,[62] there are national regulations, standards, and guidelines for health information security, especially in the electronic environment. These rules provide health care organizations and other stakeholders with a comprehensive and consistent point of view regarding information security. In addition, these rules act as a comprehensive guideline for implementing information security programs in health care organizations.[48] In addition, IT governance and the IT department structure of Iran's hospitals affect upon this problem. The research carried out by Shahi[63] at ten hospitals of Iran demonstrates no framework for IT governance and IT department structure at the studied hospitals. Additionally, the findings reveal that there are problems with the IT department personnel, information security procedures, and IT policy making.[63] IT governance has a great impact on the information security policies of the organization. The main advantage of existing information governance in an organization is creation of an organizational point of view toward information security.[64] According to ISO 27799 standards, there should be an organizational point of view toward information security at hospitals. Information security needs to be an organizational activity with the participation of all employees. Information governance should be unified with clinical governance.[46] In their risk analysis model for hospital, Sunyaev and Pflug[65] also emphasize on the responsibility of the hospital management in the information security process.The main problem of the IT department structure at Iran's hospitals is the IT personnel. In none of the hospitals is the title of CISO practically specified in the organizational structure of the IT department. CISO has a key role in ISM in an organization.[66] Risk management, vulnerability assessment, and management of information security are all CISO skills.[67] Furthermore, ISRM is a complex and specialized process and therefore, for applying the major information security risk assessment and management methodologies, specialized knowledge of the executive team, including the IT personnel, is required.[55] Tavakoli et al[68] reveal that the hospitals selected by them were not familiar with specific information security standards.

The success of ISRM depends on identification of all risks and, most importantly, analysis and determination of each risk level. Depending on the risk model used, risks are identified by determining risk factors such as assets, threats, vulnerability, likelihood of occurrence, and consequences.[52] This study shows that determining the likelihood of occurrence and analysis of impact are carried out in less than one-third of the hospitals. Moreover, risk analysis and evaluation are not actually carried out in the hospitals. Determining likelihood of occurrence and analysis of impact have an important role in constructing the scenario for risk incidence and risk determination.[37] Risk analysis and evaluation form the basis for risk prioritization

Control analysis		Likelihood determination		Impact analysis		Number of hospitals
Continuous analysis of control measures	Using systematic approach to control analysis	Likelihood determination	Using systematic approach to likelihood determination	Threat consequences determination	Using systematic approach to impact analysis	
Frequency	Frequency	Frequency	Frequency	Frequency	Frequency	
105	1	75	0 Missing: 1	116	0	404
21	0	19	0	23	0	67
4	0	3	0	4	0	8
2	0	1	0	4	0	12
32	1	19	0	20	0	58
164	2	117	0 Missing: 1	167	0	549

as well as decision making about risk treatment.[69] In addition, determining likelihood of occurrence, impact analysis, and risk analysis and evaluation require the use of precise quantitative or qualitative methods because it is more complicated, as compared with other stages of risk management. Accordingly, a variety of tools, examples, and methods are usually provided in risk assessment and management standards and methodologies for their accurate measurement.[55] One reason for this weakness at the studied hospitals could be lack of specific methodologies and standards for risk assessment and management. Some other studies also indicate a weakness in ISRM in hospitals.[54,70]

The main approach of hospitals for risk reduction is implementation of basic control measures of information security, which includes a set of management, technical, and physical conservation for information security protection. Some of the studies also indicate the implementation of basic control measures of information security.[68]

Conclusion

There is a great distance between activities carried out in Iran for ISRM and the common and standard activities of ISRM in practice. There is no appropriate and standard approach to ISRM at Iran's hospitals. This study suggests using specific information security standards such as ISO 2700x series as an effective method in the case of ISRM implementation. Considering the lack of specific national laws for health information protection in Iran, ISRM should be addressed comprehensively in a review of Iranian Hospitals Accreditation Standards. For a better performance of these cases, they should comply as much as possible with the standards of ISO 2700x series such as ISO 27799.

To help in risk calculation, based on the methodologies and specialized tools of information security risk assessment and risk management, a computer program should be designed by the Ministry of Health of Iran to calculate the risk and this should be made available to the hospitals. Moreover, hospitals should be asked to plan their ISM based on professional standards of information security such as ISO 2700x series.

Acknowledgments

This study was part of a PhD dissertation supported by the Iran University of Medical Sciences (grant number IUMS/SHMIS-1391/489). The authors thank the Office of Hospital Management and Clinical Service Excellence, Vice-Chancellor for Treatment, and the Ministry of Health of Iran for contributions to the study.

Author contributions

FS supervised the group, contributed to the first and the final drafts, and supervised the analysis of data. JZ designed the study, wrote the first draft and contributed to the final draft, collected data, and conducted the analysis.

Disclosure

The authors report no conflicts of interest in this work.

Table 4 Information security risk analysis and evaluation in hospitals

Type of ownership	Risk analysis			
	Assessment of incidence scenarios	Using systematic approach to assessment of incidence scenarios	Impact estimation	Using systematic approach to impact estimation
	Frequency	Frequency	Frequency	Frequency
Universities of Medical Sciences	0	0	4	0
Private	0	0	1	0
Military	0	0	0	0
Charity	0	0	0	0
Other organizations	0	0	2	0
Total	0	0	8	0

Table 5 Information security risk treatment and risk acceptance in hospitals

Type of ownership	Define criteria for risk treatment and risk acceptance		Risk treatment	
	Define criteria for risk treatment option and action plan	Define criteria for residual risk acceptance	Risk reduction by using comprehensive risk treatment action plan	Risk reduction by implementation of basic security control measures
	Frequency	Frequency	Frequency	Frequency
Universities of Medical Sciences	0 Missing: 2	0		389 Missing: 2
Private	0	0	0	65
Military	0	0	0	8
Charity	0	0	0	7
Other organizations	1	0	0	51
Total	1 Missing: 2	0	0	520 Missing: 2

Table 6 Continuous monitoring and reviewing of ISRM in hospitals

Type of ownership	Information security policy and procedure	ISRM policy and procedure	Risk factors	Risk management process	Implementation of security control measures	Residual risks	Using systematic approach to ISRM monitor and review	Number of hospitals
	Frequency	Frequency	Frequency	Frequency	Frequency	Frequency	Frequency	
Universities of Medical Sciences	91 Missing: 2	2	0	2	89	2	0	404
Private	18	1	0	1	17	0	0	67
Military	5	0	0	0	5	0	0	8
Charity	5	0	0	0	5	0	0	12
Other organizations	27	1	0	1	26	3	0	58
Total	146 Missing: 2	4	0	3	142	5	0	549

Abbreviation: ISRM, Information Security Risk Management.

		Risk evaluation				Number of hospitals
Determination of the level of risk	Using systematic approach to determination of the level of risk	Risk evaluation	Using systematic approach to risk evaluation	Prioritization of risks	Using systematic approach to prioritization of risks	
Frequency	Frequency	Frequency	Frequency	Frequency	Frequency	
3	0	3	0	81	0	404
1	0	1	0	18	0	67
0	0	0	0	4	0	8
0	0	0	0	2	0	12
4	0	4	0	18	0	58
0	0	8	0	124	0	549

	Residual risk Identification and acceptance			Number of hospitals
Using systematic approach to risk treatment	Identification of residual risks	Residual risk acceptance and remedy	Using systematic approach to residual risk Identification and acceptance	
Frequency	Frequency	Frequency	Frequency	
0	4	3	0	404
0	2	0	0	67
0	2	0	0	8
0	0	0	0	12
0	4	3	0	58
0	13	6	0	549

References

1. Meier CA, Fitzgerald MC, Smith JM. eHealth: extending, enhancing, and evolving health care. *Annu Rev Biomed Eng*. 2013;15:359–382.
2. Bloomrosen M, Starren J, Lorenzi NM, Ash JS, Patel VL, Shortliffe EH. Anticipating and addressing the unintended consequences of health IT and policy: a report from the AMIA 2009 Health Policy Meeting. *J Am Med Inform Assoc*. 2011;18(1):82–90.
3. Fichman RG, Kohli R, Krishnan R. Editorial overview-the role of information systems in healthcare: current research and future trends. *Inform Syst Res*. 2011;22(3):419–428.
4. Aghazadeh S, Aliyev A, Ebrahimnezhad M. Review the role of hospital information systems in medical services development. *Int J Comput Theory Eng*. 2012;4(6):866.
5. Aghajari PE, Hassankhani H, Shaykhalipour Z. Healthcare information system: The levels of computerization. *Intl. Res. J. Appl. Basic. Sci*. 2013;7(9):536–540.
6. Meingast M, Roosta T, Sastry S, editors. Security and privacy issues with health care information technology. *Engineering in Medicine and Biology Society, 2006 EMBS'06 28th Annual International Conference of the IEEE*. New York, NY: IEEE; 2006.
7. Samy GN, Ahmad R, Ismail Z, editors. Threats to health information security. *Information Assurance and Security, 2009 IAS'09 Fifth International Conference on*. Xi'an: IEEE; 2009.
8. Hoffman S, Podgurski A. In sickness, health, and cyberspace: protecting the security of electronic private health information. *Boston Coll Law Rev*. 2007;48(2):06–15.
9. Fernández-Alemán JL, Señor IC, Lozoya PA, Toval A. Security and privacy in electronic health records: a systematic literature review. *J Biomed Inform*. 2013;46(3):541–562.
10. New Zealand Ministry of Health. *Health Information Security Framework Essentials and Recommendations. HISO 100291*. Wellington: New Zealand Ministry of Health; 2009.
11. Jouini M, Rabai LBA, Aissa AB. Classification of security threats in information systems. *Procedia Comput Sci*. 2014;32:489–496.
12. NIST. Special Publication 800-30-Revision 1. Guide for Conducting Risk Assessments. Gaithersburg: NIST; 2012.
13. Myler E, Broadbent G. ISO 17799: standard for security. *Inf Manage*. 2006;40(6):43.
14. Whitman M, Mattord H. *Management of Information Security*. 4 ed. Boston: Cengage Learning; 2013:576.
15. enisa [webpage on the Internet]. Risk Management/Risk Assessment European Union Agency for Network and Information Security (ENISA); 2005–2014 [cited May 11, 2014]. Available from: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management. Accessed March 11, 2014.
16. Fenz S, Ekelhart A, Neubauer T. Information security risk management: in which security solutions is it worth investing? *Commun Assoc Inform Syst*. 2011;28(1):329–356.

17. Humphreys T. Information Security Risk Management Handbook: Handbook for ISO/IEC 27001. London: British Standard Institution; 2010.
18. Dubois É, Heymans P, Mayer N, Matulevic˘ius R. A systematic approach to define the domain of information system security risk management. In: Nurcan S, Salinesi C, Souveyet C, Ralyté J. *Intentional Perspectives on Information Systems Engineering*. Berlin: Springer; 2010:289–306.
19. Silva MM, de Gusmão APH, Poleto T, e Silva LC, Costa APCS. A multidimensional approach to information security risk management using FMEA and fuzzy theory. *Int J Inform Manag*. 2014;34(6):733–740.
20. Wager KA, Wickham Lee F, Glaser JP. Managing Health Care Information System: A Practical Approach for Health Care Executives. Hoboken: John Wiley & Sons; 2005.
21. Stoneburner G, Goguen A, Feringa A. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology, Gaithersburg: Booz Allen Hamilton Inc. 2002.
22. Nikpajuh A, Karimi AA. *Health Promotion in Hospitals: Evidence and Quality Management*. Tehran: Institute for modern Iranian Health Promotion and Disease Prevention; 2010. (In Persian).
23. Ministry of Health and Medical Education. *Report of Use of Hospital Information Systems in Iran*. Tehran: Ministry of Health and Medical Education; 2014. (In Persian).
24. Akhondzade R. Health system transformation project, an opportunity or a threat for doctors (Editorial). *J Anesthesiol Pain*. 2014;5(1):1–2. (In Persian).
25. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security requirements and solutions in electronic health records: lessons learned from a comparative study. *J Med Syst*. 2010;34(4):629–642.
26. Fildes J. Stuxnet Virus Targets and Spread Revealed: BBC News; February 15, 2011; [cited February 18, 2014]. Available from: http://www.bbc.com/news/technology-12465688. Accessed on February 18, 2014.
27. Munro K. Deconstructing flame: the limitations of traditional defences. *Comput Fraud Secur*. 2012;2012(10):8–11.
28. Demidov O, Simonenko M. Flame in cyberspace. *Secur Index*. 2013;19(1):69–72.
29. Wangen G. The role of malware in reported cyber espionage: a review of the impact and mechanism. *Information*. 2015;6(2):183–211.
30. GReAT. *The Regin Platform: Nation-State Ownage of GSM Networks*. Moscow: Kaspersky Lab's Global Research & Analysis Team (GReAT); 2014.
31. Symantec. Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance. Cupertino, CA: Symantec Corporation; 2014.
32. ISO. ISO/IEC 27005. Information Technology – Security Techniques – Information Security Risk Management (First Edition). Geneva: International Organization for Standardization; 2008.
33. Caralli RA, Stevens JF, Young LR, Wilson WR. Introducing octave allegro: Improving the information security risk assessment process. Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2007 Contract No.: CMU/SEI-2007-TR-009.
34. CLUSIF. Risk Management- Concepts and Methods. Paris: CLUSIF; 2010.
35. CLUSIF. MEHARI 2010 Processing Guide for Risk Analysis and Management. Paris: CLUSIF; 2011:1–32.
36. Ministry of Finance and Public Administration. *MAGERIT – Version 3.0. Methodology for Information Systems Risk Analysis and Management*. Madrid: Ministry of Finance and Public Administration-Technical Secretariat, Information, Documentation and Publications Unit Publications Center; 2014.
37. Ferderal Office for Information Security B. Supplement to BSI-Standard 100-3. Application of the Elementary Threats from the IT-Grundschutz Catalogues for Performing Risk Analyses. Bonn: Ferderal Office for Information Security B; 2011.
38. Communications Security Establishment Canada. editor. *Overview: IT Security Risk Management: A Lifecycle Approach (CSEC ITSG-33)*. Canada: Communications Security Establishment Canada (CSEC); 2012.
39. SOMAP.org. Open Information Security Risk Assessment guide, Version 10. The Security Officers Management and Analysis Project (SOMAP.org); 2007:1–35, Available from: http://download.matus.in/security/Open%20Information%20Security%20Risk%20Assessment%20Guide_v1.0.0.pdf. Accessed February 8, 2014. Accessed on February 26, 2014.
40. Casey T. Threat Agent Library Helps Identify Information Security Risks. Intel White Paper, September; 2007.
41. Lund MS, Solhaug B, Stølen K. *Model-Driven Risk Analysis: The CORAS Approach*. Berlin: Springer; 2010.
42. ETSI. Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN): Methods and protocols. Part 1: Method and Proforma for Threat, Risk, Vulnerability Analysis(TVRA). France: European Telecommunications Standards Institute (ETSI); 2006:1–100.
43. The Open Group. *Open Group Standard. Risk Analysis (O-RA)*. Berkshire: The Open Group; 2013.
44. ANSSI. EBIOS 2010 – Expression of Needs and Identification of Security Objectives. France: ANSSI; 2014 [cited October 1, 2014]. Available from: http://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf. French
45. ISO. ISO/IEC 17799:2005. Information Technology – Security Techniques – Code of Practice for Information Security Management. Geneva: International Organization for Standardization; 2005.
46. ISO. ISO 27799:2008(E). Health Informatics-Information Security Management in Health Using ISO/IEC 27002. Geneva: International Organization for Standardization; 2008.
47. Tritilanunt S, Tongsrisomboon A. Risk analysis and security management of IT information in hospital. *Int J Comput Inform Technol*. 2014;4(3):1–9.
48. Mortaza MB. Risk management for health information security and privacy. *Am J Health Sci*. 2012;3(2):125–134.
49. Macedo FN. Models for assessing information security risk, MSc thesis, Instituto Superior Técnico da Universidade Técnica de Lisboa, 2009.
50. Van Deursen N, Buchanan WJ, Duff A. Monitoring information security risks within health care. *Comput Secur*. 2013;37:31–45.
51. Shahri AB, Ismail Z. A tree model for identification of threats as the first stage of risk assessment in HIS. *J Inform Secur*. 2012; 3(2):169.
52. Jansen A. The cyber security risk assessment maturity of hospitals, MSc thesis, Institute of Information and Computer Science, Utrecht University, 2014.
53. Bava M, Cacciari D, Sossa E, Zotti D, Zangrando R, editors. Information security risk assessment in healthcare: the experience of an Italian Paediatric Hospital. *Computational Intelligence, Communication Systems and Networks, 2009 CICSYN'09 First International Conference on*. Indore: IEEE; 2009.
54. Temesgen DK. Analysis of The Health Information Security Management Practices of Healthcare Organizations in Amhara Region, Ethiopia the Case of Felege Hiwot Regional Referal, MSc thesis, The School of Graduate Studies of Addis Ababa University, 2011.
55. Technical Department of European Network and information Security Agency (ENISA), Section Risk Management. *Risk Management: Implementation Principles and Inventories for Risk Management/ Risk Assessment Methods and Tools*. Greece: Technical Department of European Network and information Security Agency (ENISA), Section Risk Management; 2006.
56. Kouns J, Minoli D. Information Technology Risk Management in Enterprise Environments. Hoboken: John Wiley & Sons, Inc; 2010.
57. Pandey SK, Mustafa K. A comparative study of risk assessment methodologies for information systems. *Bull Electr Eng Inform*. 2012;1(2):111–122.
58. Razavi H, Mohaghegh M, EmamiRazavi S. *Hospital Accreditation Standards in Iran*. Tehran: Ministery of Health & Education; 2011. (In Persian).

59. The ISO 27000 Directory [webpage on the Internet]. An Introduction to ISO 27001, ISO 27002.ISO 27008. The ISO 27000 Directory; 2014 [cited May 25, 2014]. Available from: http://www.27000.org/index.htm. Accessed May 25, 2014.
60. Moghaddasi H, Hosseini AS, Sajjadi S, Nikookalam M. Reasons for deficiencies in health information laws in Iran. *Perspect Health Inf Manag*. 2014;11:1b.
61. Foster B, Lejins Y, editors. Ehealth security Australia: the solution lies with frameworks and standards. 2nd Australian eHealth Informatics and Security Conference; 2013 2nd-4th December; Edith Cowan University, Perth, Western Australia. Perth: SRI Security Research Institute; 2013.
62. Garner JC. Final HIPAA security regulations: a review. *Manag Care Q*. 2003;11(3):15–27.
63. Shahi M. Proposed framework for information technology governance in hospitals affiliated to Iran University of Medical Sciences, PHD Thesis, Tehran, Iran University of Medical Sciences, 2014. (In Persian).
64. Posthumus S, Von Solms R. A framework for the governance of information security. *Comput Secur*. 2004;23(8):638–646.
65. Sunyaev A, Pflug J. Research toward the practical application of a risk evaluation framework: Security analysis of the clinical area within the German Electronic Health Information System. Proceeding in: 24th Bled e-Conference e-Future: Creating Solutions for the Individual, Organizations and Society; June 12–15; 2011, Bled, Slovenia. Association for Information Systems Electronic Library (AISeL); 2011, 156–68.
66. Johnson ME, Goetz E. Embedding information security into the organization. *IEEE Secur Privacy*. 2007;5(3):16–24.
67. Whitten D. The chief information security officer: an analysis of the skills required for success. *J Comput Inform Syst*. 2008;48(3):15.
68. Tavakoli N, Ehteshami A, Hassanzadeh A, Amini F. Information security management in Isfahan University of Medical Sciences' Academic Hospitals in 2014. *Int J Health Syst Disaster Manag*. 2014;2(3):175.
69. Bahti H, Regragui B. Risk management for ISO 27005 decision support. *Int J Innov Res Sci Eng Technol*. 2013;2(3):530–538.
70. Landolt S, Hirschel J, Schlienger T, Businger W, Zbinden AM. Assessing and comparing information security in Swiss Hospitals. *Interact J Med Res*. 2012;1(2):e11.