IIOAB JOURNAL

ARTICLE

THREATS AND SOLUTIONS FOR THE SECURITY OF ELECTRONIC PATIENT RECORD (EPR) IN A DEVELOPING COUNTRY

Mehdi Kahouei[1*], Jamileh Mahdi Zadeh[2], Zainab Abbasi[3]

[1]*Social Determinants of Health Research Center, Nursing and Allied Health School, Semnan University of Medical Sciences, Semnan, IRAN*

[2]*Medical School, Semnan University of Medical Sciences, Semnan, IRAN*

[3]*Student Research Committee, Nursing and Allied Health school, Semnan University of Medical Sciences, Semnan, IRAN*

ABSTRACT

Introduction: *The current policy of the Ministry of Health of Iran is to make an extensive use of information technology in the field of health and establish Electronic Patient Records (EPR). Therefore, addressing the issue of information security is of great importance. This study raised questions such as what threats to and solutions for the security of EPR are proposed and prioritized by the health care staffs.* ***Methods:*** *This cross-sectional study was conducted on 400 employees of hospitals affiliated to Semnan University of Medical Sciences of Iran. A valid, reliable and anonymous self-administered questionnaire was used in this study.* ***Results:*** *Mean score of human factors was 2.63 and of system defects was 1.96 as EPR threats. 86(36.6%) of the participants selected codified programs, 72(30%) of them chose managerial supports, 51(21.4%) of the study subjects selected continuous monitoring and 41(17.3%) chose the development of standards as the first priorities of the EPR security solutions. Resistance in new technology acceptance and inadequate education had significant and direct relationships with the threat of human factors (B=0.359, P<0.001) (B=0.521, P<0.001). Technical factors had significant and direct relationship with the threat of systemic defects (B=0.464, P<0.001).* ***Conclusion:*** *Administrators, developers, and analysts of information systems in health care organizations can use these results not only to establish information systems, but also to pay more attention to the different dimensions of EPR security. In addition, they can train the staffs, to promote the organizational culture.*

KEY WORDS
Threatening, Solution, Security, Computerized Patient Medical Records, Iran

Published: 10 October 2016

***Corresponding Author**
Email:
mkahouei@yahoo.com
Tel.: ++989127313543

INTRODUCTION

Along with the development of information technology, it is of great importance to consider the security threats and the methods to deal with them in this field. Nowadays, computer networks are extensively used for the exchange of critical data between different geographic locations; although it has many benefits for mankind, it has created a vast field for abuse. Therefore, one of the most important issues in the field of information technology is the security of information technology [1-3], which aims to keep the health information confidential, while at the same time keep it integrated and highly accessible [4,5]. In addition, authorized access to the information in the field of health care is one of the most important indicators of information security [6,7]. Health care consumers are worried about health care information technology and electronic health records as they may make patients' personal health information more accessible to a wide range of people [7, 8]. Studies suggest that the most of people have concerns about the unauthorized disclosure of their personal information and are worried about the share of information on websites [9, 10]. As a consequence, concerns about the security and confidentiality of data have become the biggest obstacle to the widespread implementation of computerized electronic records and hindered the distribution of data [11]. In small organizations it may be simple to ensure the security of data, as every person has the responsibility to secure his / her own computer and files. However, for larger organizations, such as health care organizations, that store the confidential personal and medical data of patients, there is a more strong need to establish formal security policies and procedures [12-14]. According to the results of many studies, the most of organizations stated that they keep the information secure as they are firstly trying to reduce the related risks. Moreover, some of organization reported that training employees and raising their awareness were the main measures taken to ensure information security. In addition and some of organizations said they were not able to appropriately respond to security events [15-18]. Currently, there is an increasing use of computer networks either via LAN (local area network) or WAN (wide area network) in the public sector and particularly in organizations that digitally register much of their important information; however, the security of information exchange environment is not desirable [19, 20]. While designing and developing clinical information systems, it should be noted that health care workers are key elements in the system, because the employees can understand and evaluate the needs of these systems, and thus develop and implement solutions. In fact, the staffs are the main agents running such systems. Therefore, a successful information system should evaluate and consider the needs of the intended users and the type and scope of their activities [21-23]. Before the design and development of computer information systems, there should be a careful analysis of the needs of organizations and users; it provides an opportunity and lets the designers and developers of such systems and other health care providers to determine their needs for changing or developing an information system. Also, if possible, it can be used to detect the amendable deficiencies in the existing system of health care [24]. The current policy of the Ministry of Health and Medical Education of Iran is to make an extensive use of information technology in the field of health and medical information, implement hospital information systems in the majority of hospitals, make electronic connections between hospitals, and establish electronic patient records. Therefore, addressing the issue of information security is of great importance. Given that few studies have been conducted so far to prioritize the staff's views toward

Electronic Patient Records, the researchers in this study raised the following question: what challenges to and solutions for the security of Electronic Patient Records are proposed and prioritized by the health care staffs. To find the answer to this question we conducted this study aimed to determine the challenges to and solutions for the security of Electronic Patient Records.

METHODS

A cross-sectional survey was performed on employees who were working in hospitals affiliated to Semnan University of Medical Sciences, Iran. The research was performed from December 2014 to October 2015. All clinical and non-clinical staff (n=400) was included in this study. In these hospitals, transition from paper medical records to EPR started in 2007 and was completed in 2010. Before the introduction of this system, all of them had been trained on EPR. An anonymous self-administered questionnaire was developed after reviewing EPR literatures. It was divided into four areas: 1) demographics, such as gender, age, job, education and job experience; 2) Challenges of EPR security such as resistance in the acceptance of new technologies, Insufficient training and awareness, lack of necessary laws and regulations technical factors; 3) Threats of EPR such as Human factors, environmental factors and system defects. In second and third sections, the study subjects' answers were graded as low=1, somewhat =2, high=3 and very high=4 respectively; 4) Solutions such as codified programs, managerial support, development of standards and continuous monitoring. The participants were asked to prioritize their views from 1 to 4 in order to the importance of the solutions. The primary questionnaire was reviewed for content validity (through the content validity index (CVI)), and then evaluated by 10 experts, who offered feedback in relation to the simplicity and clarity of questions, and the relationship between questions. The experts evaluated each question on a 4-point scale (1=low score; 4=high score), and the ratio of their response scores (3 and 4 to the total of 10 responses) were obtained. Items with scores higher than 0.80 were considered suitable; items with scores of less than 0.80 were removed or revised as recommended by the experts, and then reevaluated. Of the original 21 items, 17 were selected to form the questionnaire for this research, which was then pilot tested on 22 employees, randomly selected from the hospitals. Based on their responses, further revisions were made and some items rephrased. Internal consistencies were expressed as Cronbach's alpha 0.866 for the second area, 0.738 for the third area, 0.877 for the fourth area and 0.824 for the entire questionnaire. Next, further revisions were made and some statements were rephrased. Lastly, the final version of the anonymous questionnaire was distributed among the study subjects who were working in the hospitals by the researcher and they were asked to complete the questionnaire. To determine the distributions of responses, SPSS was used to perform descriptive statistics for all demographic variables. A total attitude score was calculated by mean of the scores for some items (low score = mean<3 and high score = mean>=3). Regression was used to investigate effective factors on EPR security. The significance level was set at $P<0.05$. First, we obtained ethical approval from the Semnan University of Medical Ethics Committee. Then, we prepared a cover letter describing the purposes of the study. The letter explained that responding to the survey indicated the participants' consent to take part in the research. It also assured the participants that all responses would be kept confidential.

RESULTS

A total of 400 questionnaires were distributed; 280 were returned, which represented a response rate of 62.5%. There were 174(69.6%) female, the sample was typically young (55.2% under 30 years of age), 147(63.9%) had bachelor degree, 140 (59.6%) were clinical staffs. [Fig. 1] shows that insufficient training achieved high score (mean=3.11) and technical factor gained low score (mean=2.24) of the study subjects' attitudes towards challenges of EPR security.

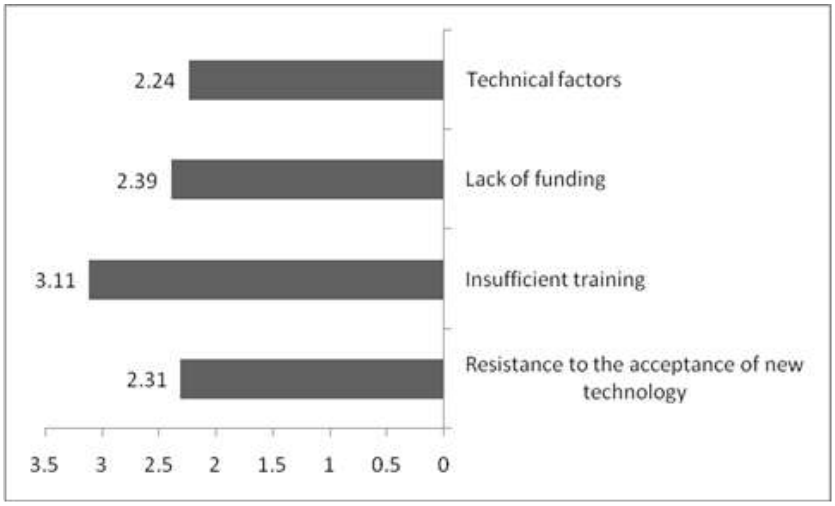

Fig. 1: Mean scores of the study subjects' attitudes towards challenges.

[Fig. 2] shows Mean scores of the study subjects' attitudes towards EPR threats. Mean score of human factors was 2.63 and of system defects was 1.96.

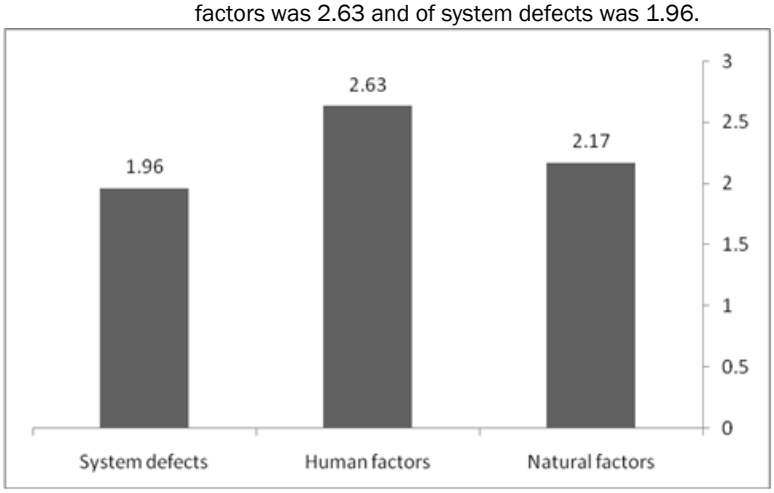

Fig. 2: Mean scores of the study subjects' attitudes towards threats.

[Table 1] has prioritized the participants' attitudes towards the EPR security solutions. 86(36.6%) of the participants selected codified programs, 72(30%) of them chose managerial supports, 51(21.4%) of the study subjects selected continuous monitoring and 41(17.3%) chose the development of standards as the first priorities of the EPR security solutions.

Table1: The participants' prioritization about effective solutions for EPR security

Priorities / Solutions	First	Second	Third	Fourth
	N (%)	N (%)	N (%)	N (%)
Codified programs	86(36.6)	48(20.4)	51(21.7)	50(21.3)
Managerial supports	72(30)	66(27.5)	59(24.6)	43(17.9)
Continuous monitoring	51(21.7)	73(30.6)	73(30.6)	41(17.1)
the development of standards	41(17.1)	46(19.5)	52(21.9)	98(41.5)

Resistance in new technology acceptance and inadequate education had significant and direct relationships with the threat of human factors (B=0.359, P<0.001)(B=0.521, P<0.001). [Table 2]

Table 2: Regression analysis challenges of the resistance in new technology adoption and inadequate training with threaten of human factors

Challenges	R^2	Adjusted R^2	F	B	SD	Beta	t	P-Value
The resistance in new technology adoption	0.492	0.490	226.980	0.359	0.024	0.709	15.066	P<0.001
Inadequate training	0.792	0.791	929.739	0.521	0.170	0.890	30.492	P<0.001

Technical factors had significant and direct relationship with the threat of systemic defects (B=0.464, P<0.001). [Table 3]

Table 3: Regression analysis challenges of technical factors with threaten of system defects

Challenges	R^2	Adjusted R^2	F	B	SD	Beta	t	P-Value
Technical factors	0.684	0.983	497.835	0.464	0.21	0.827	22.312	P<0.001

DISCUSSION

The findings of this study showed that resistance to the acceptance of new technologies is somewhat a challenge to EPR security (mean=2.31). The results may indicate that staff's resistance to new technologies might be an important factor which created a sense of distrust in cyberspace. The results of regression analysis showed that the threat of human factors to EPR security is significantly (P<0.001) due to staff's resistance to new technologies. In other words, staff's resistance to new technologies can happen when employees are not inclined to learn how to work with the new technologies and thus some of them feel unsecure facing these changes [25, 26]. Such a situation increases the risk of errors when they use EPR systems and consequently reduces the security of EPR. In addition, studies have also shown that one of the challenges of the electronic official systems is the lack of confidence and lack of interest in automation of processes. On the other hand, self-esteem, and personal experiences, and security culture of staff, compared with technical factors, are more effective and put a larger impact on the security of information systems [27, 28].

The results of this study showed that insufficient trainings and low awareness of staff about security issues (B=0.521) was among the other factors that could significantly increase the security of EPR (P<0.001). In addition, this study showed that inadequate training was among the most important challenges of staffs to secure EPR (mean=3.11). Previous studies have shown that training the staffs is one of the most powerful mechanisms for reducing the security risks [29, 30]. Elahi conducted a research and found that training and informing the users is a basic and fundamental topic for strengthening security programs, and governmental agencies must pay special attention to this gap [31]. The results also show that if organizations fail to notice the effects of trainings on staff awareness and on raising their sense of responsibility to protect the security of information, the staff will not consider themselves as a part of the process of implementation and monitoring information systems. Moreover, according to Ashenden, the human threats to information security are largely ignored. In addition, he found that to solve this problem, it is necessary to change the organizational culture and make effective communication between information security managers, senior managers, and end-users [32].

The results showed that economic factors were among the other security challenges facing EPR security (mean=2.39). It seems that the studied staff paid a special attention to the financial problems facing health centers and the high cost of purchasing equipments (software and hardware), because the limitation in financial resources is one of the common challenges facing all organizations [33]. On the other hand, there are many concerns about hospital costs and it has affected all medical centers in the world [34]. Kiel conducted a research in 2010 and studied the implementation of HIPAA security standards in several health care centers. He found that managers of health care centers at first considered the security standards as very expensive; however, a few years after the implementation of the program, they considered the standards as cost effectiveness [35].

The results showed that the technical factors were among the other EPR security concerns of the staff (mean=2.24). According to the views of the staff, technical factors play an important role in addressing security issues. The results of this study showed that neglecting technical factors can significantly (P<0.001) increase the effects of systematic defects in the system and change them into a threat to the security of EPR (B=0.464). Kayworth conducted a study and found that most organizations considered technical factors as the immediate answers to their security problems [36]. On the other hand, various studies have shown that although a small amount of security issues were related to technical factors, most organizations reported technical factors as a priority for investment in information security [37].

The results showed that a third of the studied population reported the codified programs as the most effective solution for strengthening health information security. Thus, it seems necessary to make planning to reduce duplicated tasks and prevent the waste of resources and opportunities. In a study by Xiao it was found that the lack of written and compulsory laws to regulate the electronic activities and transactions is one of the major obstacles, particularly in the public structures [4]. As a consequence, if organizations and health care institutions do not have a systematic plan for securing and protecting the data of patients, in case of the loss of sensitive information of patients, they will face much difficulty to retrieve them [14].
More than half of the studied people reported the managers' commitment and support for information security programs as the first and second priorities. Probably, the staff believed that the active involvement and support of the management were essential for achieving the success. It might be due to the fact that, information security has a strong management dimension in which some aspects like policy and management participations are very important [24]. Despite the use of several applied software, such as hospital information systems, in health centers, there is an urgent need to identify various aspects of management and their effects on patients' information security [38].

The results showed that more than half of the studied people reported the continuous and strong monitoring as the first and second priorities to prevent security problems. It is believed that the information security program must be monitored in order to correct deviations and match the activities with the objectives of information security programs. Several studies have emphasized that monitoring is one of the basic processes in the management of any organization; moreover, to correctly carry out activities in any organization it is necessary to implement a monitoring program. Using monitoring systems, organizations can achieve the maximum efficiency and effectiveness required to meet organizational goals. Bulgurcu et al. and Luna-Reyes et al. conducted studies to identify factors influencing the successful implementation of information security system. According to the results of the mentioned studies, monitoring is one of the fundamental parts of information security management. Monitoring helps to identify problems and have effective and timely responses and take more preventive measures [11, 26]. In addition, a study by Mahmoudzadeh and Rad Rajabi showed that 40% of the studied staffs reported continuous monitoring as an important factor in promoting information security [39].

A limited number of the studied staffs reported the standards and regulations as the most important solutions for promoting information security in information systems. Perhaps they considered the standards as a proper control method to prevent errors in the operations performed by the clinical information systems. It is due to the fact that, with the implementation of standards in the health care centers it is expected to observe a reduction in the number and severity of errors in the information security systems [3].On the other hand, ISO and HIPAA security standards are among the most important security standards used to protect the security of patient information [3,20]. The studies have shown that the implementation of HIPAA standard helped to effectively protect the information and made the information available only to authorized people [29, 40].

The findings of this study should be interpreted with caution because first, it was performed using self-administered questionnaires. Potential problems, such as poor understanding of the questions and possible bias, may compromise the results, but the reliability and the validity of the questionnaire established in its developmental stage may have lowered any possible impact on the results.

The results of this study showed that health care staff reported several challenges which are facing the EPR. Among them, the most important challenges were the human errors and faults and staff's lack of knowledge in the field of EPR security. On the other hand, the health center staff believed that constant monitoring of security protocols and the support of the management were among the most important solutions to strengthen EPR security. These solutions reduce the risk of damage to the information which is the most important asset of every organization. The results of this study can be much valuable for administrators, developers, and analysts of information systems in health care organizations. They may use the results not only to establish information systems, but also to pay more attention to the different dimensions of health information security. In addition, they can train the staffs, to promote the organizational culture.

CONFLICT OF INTEREST
None

ACKNOWLEDGEMENTS
We would like to thank the Clinical Research Development Unit of Kowsar and Amiralmomenin Educational, Research and Therapeutic Centers of Semnan Uiversity of Medical Sciences for providing facilities to this work.

FINANCIAL DISCLOSURE
None

REFERENCES

1. Siponen M, Vance A. [2010] Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly. 34(3):487.
2. Kahouei M, Ahmadi Z, Kazemzadeh F. [2014] Evaluation of organizational support for use of online information resources in nursing care. Journal of Evidence-Based Medicine. 7(4):252-257.
3. Farzaneh K, et al. [2011] The Survey of Job Injuries and Mental Health Disorders among Clinical Nurses from Ergonomics Aspect. Research Journal of Medical Sciences, 5(5): 289-293.
4. Xiao L, Hu B, Croitoru M, Lewis P, Dasmahapatra S. [2010] A knowledgeable security model for distributed health information systems. computers & security. 29(3):331-349.
5. Kahouei M, Alaei S, Panahi S S G S, Zadeh J M. [2014] The assessment of strategic plans of a developing country for solving barriers to access evidence-based information sources. Journal of Evidence-Based Medicine, 7(1): 45-51.
6. Stahl BC, Doherty NF, Shaw M. [2012] Information security policies in the UK healthcare sector: a critical evaluation. Information Systems Journal. 22(1):77-94.
7. Mahboobe S, et al. [2012] Mental Health and Coping Styles in Families of Epileptic Patients in Iran. The Social Sciences, 7(1): 130-133.
8. Kahouei M, Babamohamadi H, Sadat Ghazavi shariat panahi S, Mahdi Zadeh J. [2013] The impact of IT infrastructures on Iranian nurses' and students' health information-seeking strategies. Program: electronic library and information systems, 47(4): 369-383.
9. Hajrahimi N, Dehaghani SM, Sheikhtaheri A. [2013] hEALTh INfOrmATION SECurITy: A CASE STudy Of ThrEE SELECTEd mEdICAL CENTErS IN IrAN. Acta Informatica Medica. 21(1):42.
10. Mehdi K, et al. [2012] Nurses' perception about the effect of hospital information system in Iran. INFORMATION-AN INTERNATIONAL INTERDISCIPLINARY JOURNAL, 15(4): 1823-1832
11. Bulgurcu B, Cavusoglu H, Benbasat I. [2010] Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly. 34(3):523-548.
12. Williams PA. [2008] In a 'trusting'environment, everyone is responsible for information security. Information Security Technical Report. 13(4):207-15.
13. Mozhgan K, Sadat GSPS, Malekeh M, Kahouei M. [2012] The Survey of Residents and Radiologists' Attitudes about Access to Patient Information in Teleradiology in Iran. Journal of Engineering and Applied Sciences, 7(2):155-158.
14. Kahouei M, Parsania Z, Roghani PS, Firozeh M, Abadi HA. [2013] Iranian clinical staff's priorities towards the roles of health information technology and management in clinical governance. J. Eng. Appl. Sci.. 8(7):230-4.
15. Konstantinidis G, Anastassopoulos GC, Karakos AS, Anagnostou E, Danielides V. [2012] A user-centered, object-oriented methodology for developing health information systems: a Clinical Information System (CIS) example. Journal of medical systems. 36(2):437-50.
16. Safavi M, Parsania Z, Ahmadi Z, Kazemzade F, Alaei S, Sayad Jou S, et al. [2012] Mental health and coping styles in families of epileptic children in Iran. Social Sciences, 7(1):130-133
17. Kahouei M, Zadeh JM, Roghani PS. [2015] The evaluation of the compatibility of electronic patient record (EPR) system with nurses' management needs in a developing country. International journal of medical informatics. 84(4):263-270.
18. Kruger HA, Kearney WD. [2006] A prototype for assessing information security awareness. computers & security. 25(4):289-96.
19. Herath T, Rao HR. [2009] Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems. 18(2):106-25.
20. Mehdi K, Mehri F, Panoe SR, Zeinab P, Safollah A, Majid A. [2011] Evidence-based information resources management skill among Iranian residents, internship and nursing students in urgent care. Scientific Research and Essays, 6(22): 4708-4713.
21. Eminağaoğlu M, Uçar E, Eren Ş. [2009] The positive outcomes of information security awareness training in companies–A case study. information security technical report. 14(4):223-9.
22. Adler-Milstein J, Bates DW, Jha AK. [2009] US Regional health information organizations: progress and challenges. Health Affairs. 2009 Mar 1;28(2):483-92.
23. Kahouei M, Alaei S, Panahi SSG S, Zadeh JM. [2015] Strategy of health information seeking among physicians, medical residents and students after introducing digital library and information technology in

teaching hospitals of Iran. Journal of Evidence-Based Medicine, 8(2):91-97.
24. Hem Chandra MB. [2007] Financial Management Analysis of Outsourcing of the Hospital Services for Cost Containment and Efficiency: Case Study of Sanjay Gandhi Post-Graduate Institute of Medical Sciences, Lucknow, India. Journal of Financial Management & Analysis. 20(1):82.
25. Al Ameen M, Liu J, Kwak K. [2012] Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems. 36(1):93-101.
26. Luna-Reyes LF, Derrick DC, Langhals B, Nunamaker JF. [2013] Collaborative Cross-Border Security Infrastructure and Systems: Identifying Policy, Managerial and Technological Challenges. International Journal of E-Politics (IJEP). 4(2):21-38.
27. Von Solms B. [2006] Information security–the fourth wave. Computers & security.25(3):165-8.
28. Kahouei M, Kazemzadeh F, Mahdi Zadeh J, Ahmadi Z. [2016] Hierarchy of Iranian parents' information needs and social seeking behavior of infants suffering blood disease. The social Sciences, 11(3):336-342.
29. Luxton DD, Kay RA, Mishkind MC. [2012] mHealth data security: The need for HIPAA-compliant standardization. Telemedicine and e-Health. 18(4):284-8.
30. Kraemer S, Carayon P, Clem J. [2009] Human and organizational factors in computer and information security: Pathways to vulnerabilities. computers & security. 28(7):509-520.
31. Elahi Sh, Taheri M, Hasanzade A . [2009] Provide a framework for human factors related to the security of information systems. Journal of Human Sciences. 13(2):2-16.
32. Ashenden D. [2008] Information Security management: A human challenge?. Information security technical report. 13(4):195-201.
33. Komatsu A, Takagi D, Takemura T. [2012] Human Aspects of Information Security: An Empirical Study of Intentional versus Actual Behavior. InHAISA 64-74.
34. Kahouei M, Samadi F, Gazerani M, Mozafari Z. [2013] The prioritization of information needs related to health among women who had undergone surgery in obstetrics and gynecology department in hospitals of Semnan, Iran, 2012-2013. Iranian Journal of Obstetrics, Gynecology and Infertility, 16(63): 8-15
35. Kiel JM. [2010] HIPAA as standard operating procedures. Journal of Health Care Managemetnt. 29(1):80-2.
36. Kayworth T, Whitten D. [2010] Effective information security requires a balance of social and technology factors. MIS Quarterly Exec 9(3): 2012-2052.
37. Kahouei M, Eskrootchi R, Azar FEF. [2011] Understanding of Medical Students' Information Needs in Emergency Cases: The Implications for Emergency Management in Teaching Hospitals of Iran. Iranian Red Crescent Medical Journal, 13(1): 60.
38. Habibifard V. [2011] Operational Model for Information Security First congress of IT in Health. (19-21 october), Sari, Mazandaran university of medical sciences, 499-502.
39. Mahmoodzade E, Rajabi M. [2006] Security management in Information systems. Journal of Management Sciences 1(4):78-112.
40. Farzandipour M, Sadoughi F, Ahmadi MA, Karimi IR. [2008] Designing a Confidentiality Principles Model of Electronic Health Record for Iran 2007. Journal of Health Administration. 11(33):33-46.