Published online: 22/02/2015 Published print:02/2015

doi: 10.5455/aim.2015.23.39-43

ACTA INFORM MED. 2015 FEB 23(1): 39-43

Received: 21 December 2014 • Accepted: 12 February 2015

ORIGINAL PAPER

Managing the Security of Nursing Data in the Electronic Health Record

Mahnaz Samadbeik[1], Zahra Gorzin[2], Masomeh Khoshkam[3], Masoud Roudbari[4]

[1]Department of Health Information Technology, School of Allied Health professions, Lorestan University of Medical Sciences, Khoramabad, Iran
[2]Department of Health Information Technology, School of Health Management and Information Sciences, Tehran University of Medical Sciences, Tehran, Iran
[3]Department of Statistics and Mathematics, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran
[4]Anti-Microbial Resistance Research Centre, Department of Biostatistics, School of Public Health, Iran University of Medical Sciences, Tehran, Iran

Corresponding author: Zahra Gorzin, School of Health Management and Information Sciences, Shahid Yasemi Street, Valiasr Avenue, Vanak square, Tehran, Iran. Mobile: +989123740457, E-mail: Gorzin.zahra@gmail.com

ABSTRACT

Background: The Electronic Health Record (EHR) is a patient care information resource for clinicians and nursing documentation is an essential part of comprehensive patient care. Ensuring privacy and the security of health information is a key component to building the trust required to realize the potential benefits of electronic health information exchange. This study was aimed to manage nursing data security in the EHR and also discover the viewpoints of hospital information system vendors (computer companies) and hospital information technology specialists about nursing data security. **Methods:** This research is a cross sectional analytic-descriptive study. The study populations were IT experts at the academic hospitals and computer companies of Tehran city in Iran. Data was collected by a self-developed questionnaire whose validity and reliability were confirmed using the experts' opinions and Cronbach's alpha coefficient respectively. Data was analyzed through Spss Version 18 and by descriptive and analytic statistics. **Results:** The findings of the study revealed that user name and password were the most important methods to authenticate the nurses, with mean percent of 95% and 80%, respectively, and also the most significant level of information security protection were assigned to administrative and logical controls. There was no significant difference between opinions of both groups studied about the levels of information security protection and security requirements ($p>0.05$). Moreover the access to servers by authorized people, periodic security update, and the application of authentication and authorization were defined as the most basic security requirements from the viewpoint of more than 88 percent of recently-mentioned participants. **Conclusions:** Computer companies as system designers and hospitals information technology specialists as systems users and stakeholders present many important views about security requirements for EHR systems and nursing electronic documentation systems. Prioritizing of these requirements helps policy makers to decide what to do when planning for EHR implementation. Therefore, to make appropriate security decisions and to achieve the expected level of protection of the electronic nursing information, it is suggested to consider the priorities of both groups of experts about security principles and also discuss the issues seem to be different between two groups of participants in the research.

Keywords: Electronic Health Records, Management, Security, Nursing.

1. INTRODUCTION

Nursing documentation is an important part of clinical documentation (1). Nurses are the largest professional groups in hospitals and they have a long background in nursing care documentation (2). Nursing documentation is a knowledge source of patient and provable evidence demonstrating how decisions are made and decision outcomes are recorded. In other word, it really highlights what nurse do for patients (3).

Recently, introduction of new technologies has resulted in changes in health care organizations and practices. Documentation is the most important of these changes in transition from a paper-based health record to an electronic health record (EHR) (4). Using modern technologies is unavoidable in the knowledge era, Electronic Health Record (EHR) is the new technology enabling health system evolution (5). The Institute of Medicine's definition of the EHR is a set of components that form the mechanism by which patient records are created, used, stored, and retrieved and located in a health care setting (6). An EHR is used primarily for purposes of planning patient care, documenting the delivery of care and assessing the outcomes of care. In this regard, nursing documentation is an important component of EHR (7). EHR improve the quality of clinical documentation in the medical record (8). Computerized documentation will be the main mode of documentation in the future and is already used in many today's facilities (9).

Use of electronic documentation for nurses becomes relevant because this is where they acquire most of the necessary patient information (10). In this regard, information security is a critical factor for the realization and implementation of electronic health records. EHR security management is very important (11). Security is defined as the protection of system items from accidental or malicious access, use, modification, destruction, or disclosure. As well as, security management is defined as ensuring the confidentiality and privacy through controlling access to intended information (12).

Security in EHR can be seriously threatened by hackers, viruses and worms (13). In today's digital society, concerns about the privacy and security of personal data are constantly increasing, especially in healthcare (14, 15).

In addition, there is an increasing need for electronic health information exchange among patients, health care providers and payers, accordingly security and confidentiality of information systems should be considered as important success factors (16). Also, medical staff should be aware of the security measures need to protect their patient data (14). Therefore, many efforts have been made *about the* security in healthcare information systems in recent years (17). Meanwhile, it was stated that these electronic environments raise new issues of ethics, security and privacy (18). Furthermore, a series of studies suggest that the application of 'health information technology' (HIT) can actually cause security problems (19). The results of Mehraeen's study in Iran indicated that most of the hospitals had addressed issues related to information security in hospital information systems (16).

As well as, Pourasghar's study underlined that the security mechanisms for protecting medical data in HIS environment were inadequate in six university hospital in Tehran (the capital city of IRAN) and all HIS investigated suffered from lack of policies for information security, weak authentication techniques, absence of functions for managing users and log files (20). Therefore, planning and implementing more effective security policies are necessary to overcome weaknesses in different dimensions of information security (16). This study was done to explore opinions of a number of information technology specialists working in the hospital and computer company on nursing data security.

2. METHODS

This research is a cross sectional analytic-descriptive study in 2013. The study populations were IT experts at Tehran University of Medical Science's hospitals (N=10) and computer companies (N=14) in Iran. These hospitals and companies were accredited and licensed based on the SEPAS standard certificate rendered by the Statistics and Information Technology Office of the Ministry of health & Medical education, and also could represent an array of rich experiences and perspectives about nursing data security. The implementation of Electronic Health Record System (SEPAS in Persian) is the most important strategy of Ministry of Health and Medical Education in Iran. SEPAS acquire information from health care delivery facilities and accumulate. With development of this system, nursing information of individual will be integrated and available everywhere (21). Because, statistical population was limited, the whole population was studied.

Since one hospital was the designer of their hospital information system and also had the SEPAS certificate, therefore, it excluded from the companies, it was considered as hospitals group. Furthermore, three of computer companies did not complete the questionnaires, therefore, the final number of participants was 20.

Field of study	Computer companies' experts	Hospitals experts	Total
Computer Engineering	4	6	10
Information Technology (IT)	0	2	2
Medical Informatics	1	0	1
Medical Engineering	1	0	1
Other	2	2	4
Unspecified	2	0	2

Table 1. *Participants by field of study*

Data was collected by a self-developed questionnaire which was made using the results of a systematic review on security and privacy in electronic health records (13) and expert consensus. This questionnaire had two parts. The first part was related to demographic information of the participants comprising age, gender, academic discipline, educational degree, years in practice. The second part of questionnaire included 71 questions concerning security of nursing data in the electronic health record in three sections including methods of nurses' authentication in EHR documentation (8 questions), levels of information security protection (4 questions) and security requirements (59 questions). Also, an open question was included at the end of the questionnaire. Participants were asked to prioritize each question by a three point scale from "first preference" to "third preference". Each level on the scale was assigned a value starting at 1 (third preference) and ended to 3 (first preference) on the other. Due to high number of questions in security requirements, only the result of questions which were at the first priorities of the both experts, were considered.

The content validity of the questionnaire was confirmed by five specialists (two medical informaticians and three health information management). Cronbach's alpha coefficient was used to evaluate reliability of questionnaire ($\alpha \geq 0.71$ for all sections). Data analysis was performed by descriptive analytical statistics. To analysis the data, SPSS software version 18 was used.

The Comparison between two expert groups for the nurse authentication in EHR documentation (Table 2), the levels of information security protection (Table 3) and security requirements (Table 4) was calculated by independent-samples t-test (Table 3 and Table 4) and Mann-Whitney's U test (Table 2). Although, the Mann-Whitney Test could not be performed on empty variables of Table 2. A P value of < 0.05 was considered significant. The Kolmogorov-Smirnov Z test was used to determine that the distribution was normal in the groups ($P > 0.05$). The last question that appeared on the section of security requirements of the questionnaire were open-ended and allowed for qualitative analysis. Open-ended comments about this final question were reviewed independently by two authors for descriptive reporting of the comments.

3. RESULTS

The mean age of information technology experts in hospitals and computer companies' experts was 30.2 and 40.4 years respectively. The majority of information technology experts in hospitals (70%) and experts in computer companies (100%) were male. About 50% of information technology experts in hospitals had graduated in associate and bachelor degree, and 40% of experts in computer companies had bachelor degree. The mean of working experiences for information technology experts in hospitals and experts in computer companies were 5.1 and 15.5 year respectively.

As Table 2 shows, the most popular methods for authenticating users in EHR documentation is a user name and password based on experts' viewpoints.

Nurse authentication methods in EHR documentation	Main priorities of information technology experts	
	Hospitals (%)	Computer companies (%)
User name	100	90
Password	80	80
Finger print	0	0
Iris scanning	0	0
Voice	20	0
Face	20	0
Smart card	20	20
Combination of methods	0	20

Table 2. *The relative frequencies of main priorities of information technology experts in hospitals and computer companies for nurse authentication in EHR documentation*

According to levels of information security protection (Table 3), administrative and logical controls were also reported as the most important security levels by the experts in both groups.

The level of information security protection	Main priorities of information technology experts	
	Hospitals (%)	Computer companies (%)
Physical control: locks or individuals for information protection, control and supervision of the work environment and computing facilities	40	70
Administrative control: consists of defined policies, standards and guidelines for all computer systems	60	80
Logical control: using software and data for supervision and control on information access and computer system. i.e. user and password authentication	70	80
Access control: valid method for people access confirmation according to their role or function in organization	40	90

Table 3. *The relative frequencies of main priorities of information technology experts in hospitals and computer companies for the levels of information security protection*

As well as, the results of security requirements section (Table 4) indicated that some of needs in both groups had high frequency priorities (70% or over), including:

Period security update (88.9% , 90%), password management (88.9%, 70%), encrypting confidential information in information transferring process (90%, 70%), the security management of computer networks and sharing of information on these networks (70%, 80%), the applications of secure password system to prevent password cracking or possible attacks (90%, 70%), definition of authorized peoples for deleting documents in organization policies (77.8%, 90%,) data practices policy (77.8%, 70%) the application of authentication and authorization policies (88.9%,90%), access to servers by authorized people (90%, 90%), the hardware and software repair by authorized staffs and contractors (70.0%, 100%), the possibility of backup all electronic documentation and data (77.8%, 100%) based on viewpoint of experts in hospitals and computer companies respectively.

Scores of two expert groups have not significant difference for Tables 3 and 4 (**P**> 0/05).

In this research, the independent t-test was utilized to compare the mean scores of participating groups. Results indicated a non significant difference between the means of two expert group in hospital and computer company on the levels of information security protection (t (12) =.209, p = .838) and security requirements (t 12) = -.058, p = .954).

4. DISCUSSION

According to the experts' viewpoint of this research, user name and password have the highest priorities among the methods of nurse authentication in EHR documentation. Similarly, in another studies, user name and password were considered as a standard mechanism for limitation of access to important information of patients and also a working electronic signing process in the HIS (20, 22-24). Although, in today world of technology, the use of biometrics identification techniques including fingerprint, iris scanning, voice and face recognition systems have been increased to identify individuals and control access (25).

Based on Timmerman's model of creating and maintaining document data integrity in an enterprise electronic health record, three levels of security including physical, administrative and logical control are needed in security administration program. Although all the level are important but administrative control can have the most effect in the decrease of the staff errors in data integrity (12). The administrative and logical controls were also emphasized as important levels of information security in present study. Moreover, high point were assigned to the administrative dimension in information security based on viewpoint of more information technology managers of hospital studied in Iran (16).

The more comprehensive functions in EHR needs a more complex access control management model (16). Similarly, it was proved in Timmerman research that access control and audit trials are necessary to be a part of overall security program (12). Although in the present study, the both experts had not the same view about access control in the levels of information security protection. The experts of computer companies believed that access control has most priority, but hospital information technology experts believed that it has least priority among these levels. It is recommended that for final decision, both specialists group take a deep discussion to make best decision considering all aspects of nursing electronic information protection.

California department of public health has prepared information systems security requirements, some of the most important requirements, including conducting the periodic review of system security, establishing a process to review logs for unauthorized access to the system, encrypting confidential information, displaying the warning about unauthorized use of confidential information and providing role based access for authentication (26).From the experts' point of view in this research, the same requirements were also emphasized in security requirements of the nursing documentation in EHR.

Considering security measures to protect unauthorized access to electronic information was stated as main priorities for security requirements by the participant experts of this investigation. Also, according to the study of Harman and et al, implementing security measures sufficient to reduce the risks of impermissible access to electronic protected health information by unauthorized users to a reasonable and appropriate level (14). Moreover, two groups of participants were agreed

Security requirements	Main priorities of information technology experts	
	Hospitals (%)	Computer companies (%)
Periodic security update (Including Continuous updating of antivirus software in all systems)	88.9	90
password management (procedures for password creating, modifying and maintaining)	88.9	70
Policies and procedures to confirm access to electronic health information e.g. access authorization to system base on people role)	55.6	100
Audit control in system (audit trail provides accurate overview of what been done in document and by whom and when)	55.6	70
Technical security measures to protect unauthorized access to electronic information that is translating in an electronic communications network	62.5	70
Regularly review record of information system activity (such as audit logs, access reports and security incident tracking)	60	90
Periodic review of system security (to ensure the effective operation of management, operations, personnel controls and providing appropriate levels of protection)	75	60
encrypting confidential information in information transferring process base on approved encryption standard	90	70
encrypting confidential information in information storing process base on approved encryption standard	60	60
Policies and procedures to protect electronic health information from any improper change or destruction	50	80
display warning confidentiality of information in all systems containing information	55.6	50
Inactivating account after three failed attempts to log on	44.4	60
Define user roles and types to distinguish between functional and security needs	50	80
the security management of computer networks and sharing of information on these networks	70	80
Limiting privileges to information deletion in errors documents	50	90
definition of authorized people for deleting documents in organization policies (typically, a nurse should not have privilege to delete documents)	77.8	90
the policies for practice (i.e. how to data store, access and transfer)	77.8	70
the application of authentication and authorization policies	88.9	90
the applications of secure password system to prevent password cracking or possible attacks	90	70
access to servers by authorized people	90	90
the hardware and software maintain by authorized staffs and contractors	50	100
the hardware and software repair by authorized staffs and contractors	70	100
the possibility of backup all electronic documentation and data	77.8	100
Storing backup copies in a separate and secure location	66.7	100
Lack of linking computer systems to modems without suitable authority	77.8	55.6
Lack of connection modems to communication networks without authorization	88.9	55.6
Define specific restrictions for third-party access (such as insurance) to system	60	88.9
Define specific restrictions to access a nurse to the system outside the hospital (for example, access to the system from home)	80	66.7

Table 4. *The relative frequencies of main priorities of information technology experts in hospitals and computer companies for security requirements*

with items of HIPPA security checklist (27, 28). The necessity of having a written policy about all accesses to the health information was emphasized by Farzandipour and et al (29). This research proved that all experts believed as a high priority that some defined policies are needed for legal access to EHR. In addition, according to the study of Park and et al, hospitals can approach information security from feasible security requirements such as policy and regulation making. Also, it is necessary to reflect on the requirements of varied interests such as medical staff, medical consumers and other institutions for information security (30).

In the answer of open questions, two computer companies suggested other security requirements including: data classification based on information security and preventing the unauthorized computer access to the network. Likewise, these important security topics were mentioned in other studies as security requirements and policies (31-34).

5. CONCLUSION

Due to importance of health information, specially nursing information and the worry of nursing electronic information security, it is recommended to use the expert points of view in designing the national EHR system (SEPAS). In short, the experts had similar views about the_levels of information security protection and security requirements regardless of their work place. Therefore, utilizing especially similar views of participants can help in designing the system and prompting nursing electronic documentation. Nursing documentation system contains the patient care information supported with realization of appropriate security requirements. Finally, education and clear guidelines about systems security issues are important to nurses during the implementation of the system.

The knowledge of security should enhance permanently by education, consultation and function of staffs. Also, the establishment of the new field of nursing informatics is recommended to define effective strategy for improving electronic nursing documentation in collaboration with SEPAS stakeholders. This new discipline can manage the nursing information with least security damage according to the progress of information technology.

Acknowledgements: Mahnaz Samadbeik participated in design and writing the manuscript. Zahra Gorzin participated in original idea, design and data collection. Masomeh Khoshkam and Massoud Roudbari helped in statistical analysis and writing the manuscript. Authors thank all experts who participated in this study; these experts spent considerable time and effort and thus made the results possible.

CONFLICT OF INTEREST: NONE DECLARED.

REFERENCES

1. Mahler C, Ammenwerth E, Wagner A, Tautz A, Happek T, Hoppe B, et al. Effects of a computer-based nursing documentation system on the quality of nursing documentation. J Med Syst. 2007; 31(4): 274-282. PubMed PMID: 17685151.
2. Ellingsen G, Munkvold G. Infrastructural arrangements for integrated care: implementing an electronic nursing plan in a psychogeriatric ward. Int J Integr Care. 2007; 7(2). PubMed PMID: 17627295, PMC: 1894674.
3. Jefferies D, Johnson M, Griffiths R. A meta-study of the essentials of quality nursing documentation. Int J Nurs Pract. 2010; 16: 112-124. PubMed PMID: 20487056.
4. Williams F, Boren SA. The role of the electronic medical record (EMR) in care delivery development in developing countries: a systematic review. Inform Prim Care. 2008; 16(2): 139-145. PubMed PMID: 18713530.
5. Mandl KD, Kohane IS. Escaping the EHR trap the future of health IT. N Engl J Med. 2012; 366(24): 2240-2242. doi: 10.1056/NEJMp1203102. PubMed PMID: 22693995..
6. Conrad D, Schneider JS. Enhancing the visibility of NP practice in Electronic Health Records. J Nurse Pract. 2011; 7(10): 832-838. doi: 10.1016/j.nurpra.2011.04.004.
7. Häyrinen K, Lammintakanen J, Saranto K. Evaluation of electronic nursing documentation - nursing process model and standardized terminologies as keys to visible and transparent nursing. Int J Med Inform. 2010; 79(8): 554-564. PubMed PMID: 20617569.
8. Gunningberg L, Fogelberg Dahm M, Ehrenberg A. Improved quality and comprehensiveness in nursing documentation of pressure ulcers after implementing an electronic health record in hospital care. J Clin Nurs. 2009;18(11):1557-1564. doi: 10.1111/j.1365-2702.2008.02647.x. PubMed PMID: 19220607.
9. Cusack CM, Hripcsak G, Bloomrosen M, Rosenbloom ST, Weaver CA, Wright A, et al. The future state of clinical data capture and documentation: a report from AMIA's 2011 Policy Meeting. J Am Med Inform Assoc. 2013; 20(1): 134- 140. doi: 10.1136/amiajnl-2012-001093. PubMed PMCID: PMC3555335 .
10. Kelley TF, Brandon DH, Docherty SL. Electronic nursing documentation as a strategy to improve quality of patient care. J Nurs Scholarsh. 2011; 43(2): 154-162. PubMed PMID: 21605319.
11. van der Linden H, Kalra D, Hasman A, Talmon J. Inter-organizational future proof EHR systems: a review of the security and privacy related issues. Int J Med Inform. 2009; 78(3): 141-160. doi:10.1016/j.ijmedinf.2008.06.013. PubMed PMID: 18760661.
12. Timmerman R. A model for creating and maintaining document data integrity in an enterprise electronic health record (Thesis). Duluth, Minnesota, College of St. Scholastica; 2011. Available from: http://search.proquest.com/docview/897941171.
13. Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform. 2013; 46(3): 541-562. doi: 10.1016/j.jbi.2012.12.003. PubMed PMID: 23305810.
14. Harman LB, Flite CA, Bond K. Electronic health records: privacy, confidentiality, and security. Virtual Mentor. 2012; 14(9): 712-719. doi: 10.1001/virtualmentor.2012.14.9.stas1-1209. PubMed PMID: 23351350.
15. Walsh D, Passerini K, Varshney U, Fjermestad J. Legal issues in the transition to electronic records in health care. Information Systems: People, Organizations, Institutions, and Technologies. Physica-Verlag HD; 2010. doi: 10.1007/978-3-7908-2148-2_37 .
16. Mehraeen S. Information security in hospital information syatems in Beheshti and Tehran university of medical sciences (Thesis). Tehran: Tehran University of Medical Sciences, 2012.
17. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management. 2010; 6(4): 279-314. doi: 10.1504/IJIEM.2010.035624.
18. Nielsen BA, Baum RA, Soares NS. Navigating ethical issues with electronic health records in developmental-behavioral pediatric practice. J Dev Behav Pediatr. 2013; 34(1): 45-51. doi: 10.1097/DBP.0b013e3182773d8e. PubMed PMID: 23275058.
19. Samy GN, Ahmad R, Ismail Z. Security threats categories in healthcare information systems. Health Informatics J. 2010 16(3): 201-209. doi: 10.1177/1460458210377468. PubMed PMID: 20889850.
20. Pourasghar F. The role of information technology on documentation and security of medical data (Thesis). 2009.
21. Ministry of Health and Medical Education, Statistics and Information Technology Office. Electronic Health Records in Iran (SEPAS). 2011. Available from: http://behdasht.gov.ir/index.aspx?siteid=101&pageid=20430&newsview=25612.
22. Mtsha A. Documentation of nursing care current practices and perceptions of nurse a teaching hospital in Saudi Arabia (Thesis). Stellenbosch: University of Stellenbosch, 2009. Available from: http://scholar.sun.ac.za/handle/10019.1/4040.
23. Carter JH, . What Is the Electronic Health Record? In: Electronic health records. Second Edition ed. 2008. ISBN-13: 978-1930513976.
24. Group ISM. Healthcare information security today. 2013. Available from: http://docs.ismgcorp.com/files/handbooks/HIS-Survey-2012/HIS_Survey_Report_2012.pdf.
25. Bora SP, Dhumane PB. Biometric Authentication System. International Journal of Innovative Research and Development. 2012; 1(3): 49-60. Available from: http://ojms.cloudapp.net/index.php/ijird/article/view/34476.
26. California Department of Public Health (CDPH). Information systems security requirements for projects (ISO/SR1). 2008 (Cited 31 Dec 2014). Contract No. SR 1/v3.9. Available from: http://www.cdph.ca.gov/programs/cpns/Documents/Network-LIANIARFA2011-ExhibitI-S1CDPHISOProjectReq-V3-9-2008-10.doc.
27. Herold R, Beaver K. The practical guide to HIPAA privacy and security compliance. CRC Press; 2004. doi: 10.1201/9780203507353.ch5.
28. Kuckian S. Securing Electronic Data Exchanges for HIPAA Covered Entities to Ensure Greater Compliance with Security Rules: University of Oregon; 2011 (Cited 31Dec 2014). Available from: https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/11397/Kuckian-2011.pdf?sequence=1.
29. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Designing a Confidentiality Principles Model of Electronic Health Record for Iran 2007. Journal of Health Administration. 2008; 11(33): 33-46. (In Persian).
30. Park WS, Seo SW, Son SS, Lee MJ, Kim ShH, Choi EM, et al. Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. Healthc Inform Res. 2010; 16(2): 89–99. doi:10.4258/hir.2010.16.2.89. PubMed PMID: 21818429. PubMed PMCID: PMC3089859.
31. Wood CC, Lineman D. Information Security Policies Made Easy Version 11. Information Sheild, Inc.; 2009. ISBN:1881585166 9781881585169.
32. Koufi V, Malamateniou F, Prentza A, Vassilacopoulos G. A framework for privacy-preserving classification of next-generation PHR data. Stud Health Technol Inform. 2014; 202: 119-122. doi: 10.4258/hir.2010.16.2.89.
33. Yoshioka N, Washizaki H, Maruyama K. A survey on security patterns. Progress in Informatics. 2008; 5(5): 35-47. Available from: http://xn—vcsw1an4edyhh3b632d9qdkta.jp/pi/n5/5_35.pdf. Date accessed: 31 Dec. 2014.
34. Fernando JI, Dawson LL. The health information system security threat lifecycle: An informatics theory. Int J Med Inform. 2009; 78(12): 815-826. PubMed PMCID: 19783203.