Information Security : The Landscape of Management In Electronic Record

Mohd Shamim
Aligarh Muslim University, Aligarh India
E-mail: mohd.shamim@gmail.com

Abstract— Protecting information based on physical boundaries and firewall technologies are outdated and inadequate in this area. Today the more efforts to establish a successful information security practice by developing rules regulating and making the users understand how to follow the prescribed information security rules and policies also is not likely to be successful. Thus, a better understanding on holistic process of information security protection in healthcare industry is very important to manage information security management. Nowadays, the increasing role of information technology platform in organizing health information has led to the need of review on the confidentiality, privacy, and security of electronic information. The widespread use of electronic health records (EHRs) in healthcare industry is prevailing. Once information is electronically stored and shared, it opens the door for hackers and other malicious attackers to access the records.. Therefore, this paper is to scrutinize the landscape of security management elements that contribute on successful of implementing security management in healthcare industry. This paper also includes overview on identifying the simple process of security management that will helps any organization in healthcare industry to formulate, implement and manage any medical or hospital information system.

Keywords— Security threat; Security control; Information Security Management; Electronic Health Record (EHR)

Corresponding Author:

Mohd Shamim,
Aligarh Muslim University, Aligarh India,
Email: mohd.shamim@gmail.com

I. INTRODUCTION

Traditional security philosophy such as protecting information based on the creation of physical boundaries around assets and compartments or perimeters are outdated and inadequate (Pieters, 2011). Nowadays securing information systems has its grounding in human behavior, process and technology (Workman, Bommer, & Straub, 2008). This is because the insider threat problem is more elusive and perplexing than any other threat. Technical solutions also are insufficient since insider threats are fundamentally a people issue (Roy Sarkar, 2010). Electronics health record (EHR) has promised much advancement and improvement in services for many areas of the healthcare industry. It's a repository of patient data in digital form, stored, managed and exchanged securely and accessed by authorized users such as specialists, physicians, nurses, radiologist, pharmacists, laboratory technicians and patients (Häyrinen, Saranto, & Nykänen, 2008;Samy, Ahmad, &Ismail, 2009; Van Der Linden, Kalra, Hasman, & Talmon, 2009). All the patients' medical records must remain in secrecy and privacy (Lechler, Wetzel, & Jankowski, 2011; Acharya, 2010). Disclosure or misuse of patient's record can cause serious harm and implication to patients such as discrimination, stigmatization, or loss of insurance and employment (Acharya, 2010). Moreover, current security measures are not sufficient to guarantee that privacy of patients' record are fully protected (Lechler et al., 2011). The common issues include access right to data, security threats, how and when data is stored and secured of data transferred (Meingast, Roosta, & Sastry, 2006).

In addition, many efforts have been made to examine the problem and numerous security issues. This have been addressed by existing studies to find the main reason for security breaches recently (Waly, Tassabehji, & Kamala, 2012). According to L.Fuchs, G. Pernul and R.Sandhu (Fuchs, Permul,& Sandhu, 2011), there are thousands of scientific publications deal with the application of sociological role theory in the context of information security since two decades ago. This indicates that information security not just a physical boundaries or technical issues but it process that relate to people, technology and process (Jirasek, 2012). Hence, these are enormous challenges to any hospital's management in order to gain consumer trust and confidence towards services. In order to keep the patient's data secrecy and privacy, managing the information security must cope with all convolution of relations today's health care system and the increased exchange of sensitive patient's medical information. Since the complexity various information security issues in healthcare industry and only a few articles discussed on the whole process of security management, this paper aims to identify the security management elements that contribute o successful implementation of security management in EHR. Meanwhile the second

objective is to propose a generic flow model of security management elements in order for key players in healthcare industry easier to understand the entire concept of information security management in EHR.

II. RESEARCH METHOD

2.0 An Overview of Information security management

2.1 Review Stage

For the purposes of the overview information security management, the search of articles were carried out from year 2008 until October 2014. The search includes databases from Science Direct, IEEE Digital Library, ACM Digital Library, Proquest, JSTOR, PubMed and Google Scholar with the following keywords; Information Security and Privacy, Electronic Health Record and Security, Health Information system security and privacy, Electronic Medical Record security and e health and security. More than 100 relevant articles were selected. By going trough the full text of papers, there are 57 articles were found to be more related to the purpose of this paper. However, only 37 articles were reviewed in accordance with the eligibility criteria. Based on synthesize and comprehensive reviewed of these articles, this study analyzed and categorized the articles into 3 themes; People, Process and technology (Appendix 1). Furthermore, these there themes are used to identify the security elements that contribute to implementation of security management because most of the information system involved with these elements (Jirasek, 2012; Roy Sakar, 2010; Workman et al., 2008).

2.2 Information Security Management in HER.

Security is a chain and it's like a process, not a product (Waly et al., 2012). It involves well defined processes trough which designers develop security mechanism by implementing a suitable ser of controls, including policies, processes, procedures and participant from organizational structures and stakeholders (Asri, Stambul, & Razali, 2011; Fielden, 2012). According to Fielden (2010), the information security management cluster consists of several factors which includes: confidentiality, digital preservation, industry, regulation, information integrity, maturity models, reactive security models and risk management. Meanwhile, Dhillin (2001) stated that information system security research falls into four catagories: checklist, risk analysis, formal methods and soft approaches.

However, based on current literature there are many elements and factors that influence management security in EHR. This study aims to identify and propose four the most important aspects of information security management in EHR. There are security risk, policies and standard, information security process and stakeholder. Addressing these four aspects are

important in order to identify security threats, defining security control, execute security management model as shown in Figure 1.

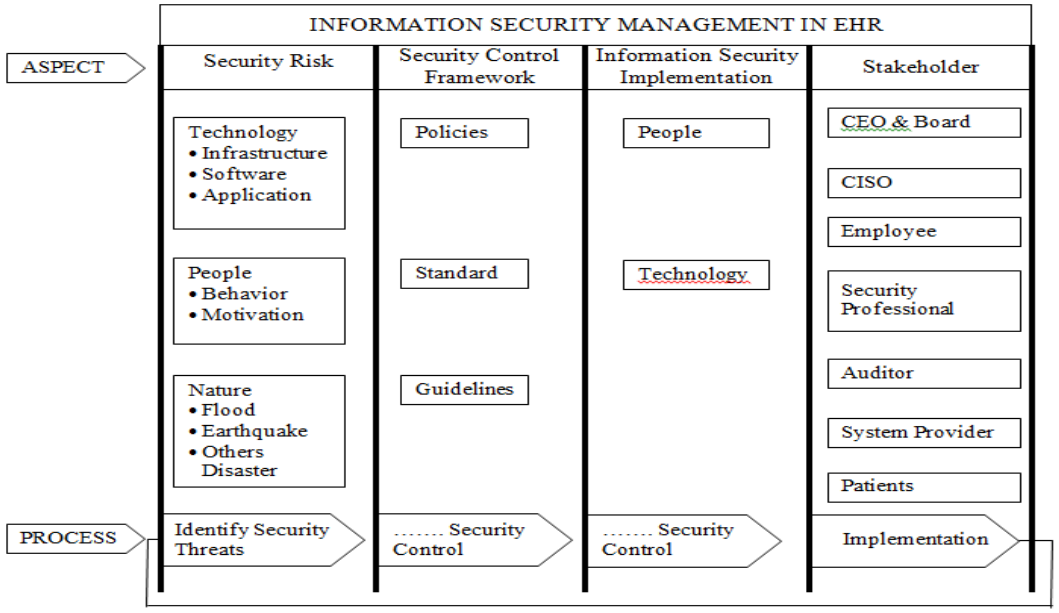

Figure 1 : Proposed Generic Information Security Management Model.

In the proposed information security management model, the process begins with identification the security risk to examine the related security threats to the system. There are three main categories of security risks which are technology, people and nature. When security threats are identified, organization may develop security control framework as well as defining security control. This process is essential to ensure organization formulate a more appropriate policy and standard that suite to the organization's nature of business. The next steps is information security implementation where people and technology are main components in this process. The technologies issued mostly related to rapid technology advancement and increasing number of cyber threats cases. The second element in information process is people while it's the most difficult elements to manage when dealing with human behavior, culture and motivation. In the last process, the stakeholder's participant during implementation of EHR system is also important to ensure the implementation of the system working as planned. However, when the system has many flaws, organization may analyze the elements on each process. The details on each element will be discussed on next section.

2.3 Security Risks

In many organizations, information security is a major concern for business including healthcare industry. A fundamental of information system security assumption is that no system is totally immune to attacks, accidents, or failures (Ahmad, Hadgkiss, & Ruighaver, 2012). Consequently, many IT companies offering solutions for viruses, malware, encryption, access control, new technologies of firewall or others physical boundaries equipments such as switches,

router or software and services to counter hackers or unauthorized users,. However, the global threats not only came from these external and internal attacks, but also from the nature such as disaster, flood and earthquake and fire. In summary, security risks can be divided into three sections;

- Technology
- People
- Nature

A. Technology

Security risks that associate with technology normally involved with infrastructures that relate to security perimeters appliances such as, firewall, routers, switches, servers and any devices an applications that applying into system management. Besides, access to the computer room that controlled by a card-based access control system, fire detection mechanisms, air-conditioning and uninterruptible power supply at facilities distribution room also parts of infrastructure (Tsohou, Kokolakis, Lambrinoudakis, & Gritzalis, 2010). Subsequently, many organizations perceive that security as expensive and costly especially with rapid changing of technologies. Moreover, the research and standardization organizations do not have enough time to analyze all possible vulnerabilities and threats before technologies are deployed (Atay & Masera, 2011). In contrast, some organizations fail to realize that investing in effective security protections will reduce in comparison to the cost of a security breach. The cost of a security breach may involve to the cost of recovery of system affected, the cost of recovery of reputational loss, and the coasts of litigation. However, organizations with limited security budgets should implement the best practice that suite to the organization in order to provide a cost effective solution. There are a lot of best practice and standards available and ISO/IEC 27001:2007 was gazetted as information security controls for all Malaysia's government agency (Malaysia, 2010).

B. People

Currently, many security breach incidents reported caused by some intentional or unintentional actions by the insiders (Crossler et al., 2013). In fact, most f surveys show that more information security breaches are caused by the actions of internal employees than by outside hackers (Humaidi, 2013). The insider actions that cause direct or indirect threats to organizational digital assets can be classified into two categories: those that are intentional, often labeled as deviant behavior such as sabotage, stealing, and industrial or political espionage. Another category is those that are unintentional, often labeled as misbehavior such as selecting a simple password, visiting non-work related websites using corporate computers, inadvertently posting confidential data onto unsecured servers or websites, or carelessly clicking on phishing links on

emails and websites (Guo, 2012;Roy Sarkar, 2010). Figure 2 shows categories of insider meanwhile figure 3 shows the motivation of human to breach the system.

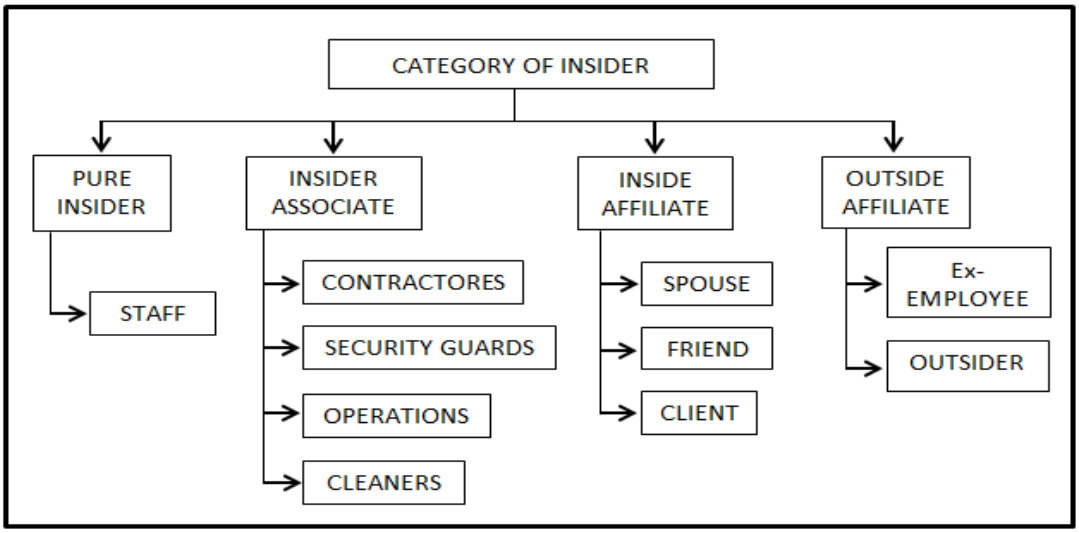

Figure 2 : Category of Insider

Source: K. Roy Sarkar, (2010)

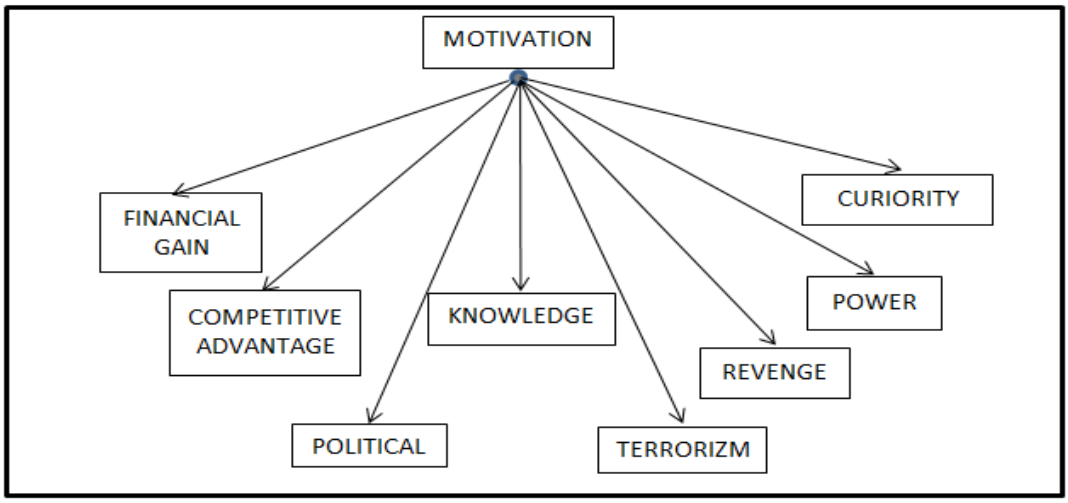

Figure 3: Motivation of people to breach system
Source : K. Roy Sarkar, (2010)

All these factors come from social environment, behavior and motivation of people. Concentrating on which information security policy contributes to the protection of information systems from internal and external threats is crucial for the organization's success (Waly et al., 2012. Thus, formulate policy and standard that based on organization culture and business objectives are important to ensure employees comply with security control.

C. Nature

Survivability of information security does not only depend on technology, people and data management but also preparation from the nature disaster such as flood, earthquake and fire. Survivability means highly protecting distributed information services and assets (Lipson & Fisher, 2000). In additional, the increased demand for continuous operation in the presence disaster become less tolerance. A remote backup can ensure continuous operation and its must works as same capacity as the primary. Hence, implementation of Business continuity management (BCM) that based on technical disaster recovery inside an organization and to identify potential risks and avoid, minimize or prepare for them as to continue business process and services without interruption is very important (Järveläinen, 2012).

2.4 Policy and Standard

Implementation of a set of policies, standards and guidelines eventually describe how the organization implement and address information security protection. All together these elements are defined as security controls (Jirasek, 2012). There are the lot of international standards available which can be source of information security controls. These can be used to develop a policy framework for each organization that suite with their nature of businesses. Nowadays, the number of standardizations. Organizations which have published information security standard that gained great acceptance include ISO. Information System Audit and Control Association (ISACA), Information Systems Security Association (ISSA), National Institute of Standards and Technology (NIST), British Standards Institution (BSI), Information Security Forum (ISF) and many more (Tsohou) et al ., 2010). Furthermore, these security standards are continuously published and gain acceptance used for guidelines, promote best practices and a few are used as basis for certification. The common well-known standard and guidelines, are ISO/IEC 27001:2005, System Security Engineering CMM (SSE-CMM), the NIST FIPS 140-2 (2001), common criteria (CC) or ISO/IEC 15408 series, COBITv4.1 (Tsohou) et al ., 2010). ISO/IEC 27001 is focused more on information security management system (ISMS) while COBIT focused on defining objective, stakeholders, maturity levels and controls (Tsohou) et al ., 2010). (Jirasek, 2012) (Existing & from 2012) Boehmer, 2008). Meanwhile Common Criteria and ITSEC focused on technical security features (Siponen & Willison, 2009). The following are definition on each element in security control framework.

- Policies - can be described as high level statement relating to the protection of information across the organization and it's also driven by legal concerns. Policies are reflect to an organization's goals, objectives, culture and intended for broad audience. They also are mandatory and applicable to anyone such as employee, contractor, temporary or third parties.

- Standard - define the process or rules to be used or implement to support the policy. Like policies, standards are mandatory and require special approval if the standard is not to be followed. Furthermore, standards promote the common understanding of security requirements and ensure that the security mechanism implemented do comply with globally accepted rules and practices.
- Guidelines - consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place. Guidelines should be viewed as best practices that are not usually requirements, but are strongly recommended. For example, a standard may require password to be 8 characters or more and a supporting guideline may state that it is best practice to also ensure the password expires after 30 days. Or guideline on how to operate firewall system.

III. RESULT AND DISCUSSION

2.5 Information Security Implementation

In any security control, policy or standard is part of process where people and technology are come into play. Each process of implementation is supported by people and also most are supported by technology (kolkowska & Dhillon, 2013).

2.5.1 Technology

Securing information technology in terms of data, hardware, and application has been the most concerned aspect since the beginning of computerized era. However, in the changing technologies cluster the following factors are considered: authentication and access, common building blocks, cyber-infrastructures, encryption, information forensics, innovative solutions, malware, mobile technologies, new architectures, parallel structures, social software and wireless technologies (Fielden, 2010). There are many tremendous efforts to secure information from illegal access, deletion, corruption, mishandling and other malicious actions. Intrusion detection systems, cryptography, and web vulnerability assessment tools (fuchsberger, 2005). Indeed, technology advancement is still the key element to protect for any security attacks. Meanwhile data management such as access control, encryption technology and authentication mechanism are also crucial part of information security process (Leitner & Rinderle-Ma, 2014). When concern over patient's health record and privacy, a few questions need to be answered (meingast et al., 2006);

- Who own the data?
- What type of data and how much data should be stored?
- Who can view a patient's medical record?
- To whom should this information be disclosed to without the patient's consent?

Therefore, the following are technical solutions exist to increase security and privacy of data access and storage.

- Role Based Access Control (RBAC); Roles are assigned to enable user to interact with the system, and determining in what situation and resource can be accessed by user (Fernandez-Aleman, Senor, Lozoya, & Toval, 2013) (Ferraiolo, Sandhhu,Gavrila, Kuhn, & Chandramouli, 2001). This is a dominant model to reduction the complexity and cost of security administration in large networked (Meingast et al., 2006).
- Encryption; Used to prevent eavesdropping and skimming and can be accomplish in hardware as well as in software (Meingast et al., 2006).
- Authentication; Authentication; used to ensure the data is coming from right person or resources. There a lot of authentication algorithm was developed such as passwords, digital signatures and challenges response authentication protocol.

2.5.2 People

Human resources, including all people working with information technology, play a significant role in information security issues. Human error is the most challenging issues in security management (Ghazvini & Shukur, 2013). The key factor for human resources in relation to information security is awareness about threats, challenges, and risks lurking in the information exchange environment (Muhaya & Minhas, 2012). Improving staff awareness of information security should be one of the significant, permanent goals in an organization's information security control (Cox, 2012). Apart of that, organization need to perform insider threat assessments in order to identify the insider threats. Every organization has a varied mix of employees, consultants, management, partners and complex infrastructure and that makes handling insider threats a daunting challenge (Roy Sarkar, 2010). There should be a limit to employees' access to sensitive data to limit negative financial impacts. Insider threats are easy to do but hard to detect, since an insider is an authorized user that makes it difficult to predict malicious activities. They are not perceived correctly because it is difficult to 'measure' as compared to an outsider attack (Roy Sarkar, 2010) (Furnell & Rajendran, 2012). Thus, new security control assessment for organization to conduct vulnerability and risk assessments and to ensure that the protection they implement is cost effective (Guo, 2012).

2.6 Stakeholder

The concept of EHR covers wide range of different information systems from departmental systems to comprehensive electronic health care records. Various kinds of departmental EHRs such as intensive care records, emergency department records or ambulatory record have now been in use for a long time.by the way, the HER is used by different health care professionals and also by administrative staff. Among the various health care professionals who use different

components of the EHR are physicians, nurses, radiologist, pharmacists, laboratory technicians and radiographers (Hayrinen et al., 2008).

Furthermore, EHRs are also used by patients or their parents, security professional, system developer and system auditors. One of the key factor that leads to effective information security management is the commitment and support from the entire stakeholders in organization (Waly et al., 2012). It is important to understand that technology is a tool that can be used or misused by people; no matter how strong the security system and policy are, they will be a threat to information security should the user fail to adhere to the policy and system (Waly et al., 2012). Thus, Chief Executive Officer, Chief Finance Officer and other stakeholders need to know that what has been promised on security control objectives are being delivered (Waly et al., 2012). More importantly the security professional need to show the value of security to business. This is the area where security professionals need to enhance their skills.

IV. CONCLUSION

The information security management model can help with ease explaining why security is important and how to manage security control. In any information security system or EHR, consideration on entire important elements in security is very important. Security is a process that needs continuously assessed. In current information age, it seems that more attention needs to be paid to security threats, information security implementation that relate to human factor and supporting from management to develop and manage security control effectively.

REFERENCES

Acharya, D. (2010). Security in Pervasive Health Care Networks: Current R & D and Future Challenges. In Eleventh international Conference on Mobile Data Management Security (pp. 305-306), doi:10.1109/MDM.2010.38

Ahmad, A., Hadgkis, J., & Ruighaver, a. B. (2012). Incident response teams – Challenges in supporting the organizational security function. Computers & Security, 31(5), 643-652, doi:10.1016/j.cose 2012 04,001

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare; current state of research International Journal of Internet and Enterprise Management, 6(4), 279 doi:10.1504/JJIEM.2010.035624

Asri, M., Stambul, M., & Razali, R, (2011). An Assessment Model of Information Security Implementation Levels. In International Conference on Electrical Engineering and informatics.Bandung, Indonesia; IEEE

Atay, S., & Masera, M, (2011). Challenges the security analysis of Next Generation Networks. Information Security Technical Report, 16(1), 3-11. doi:10.1016/j.istr.2010.10.010

Boehmer, W. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. 2008 Second International Conference on Emerging Security Information, System and Technologies, 224-231. doi:10.1109/SECURWARE.2008.7

Cheng, L., Li, Y., Li,W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security,39, 447-459. doi:10.1016/j.cose.2013.09.009

Cox, J. (2012) Information system user security: A structured model of the knowing-doing gap. Computers in Human Behavior, 28(5), 1849-1858. doi:10.1016/j.chb.2012.05.003

Cresswell, K., & Seikh, A. (2013). Organizational issues in the implementation and adoption of health information technology innovations: an interpretative review. International Journal of Medical Informatics, 82(5), e73-86 doi:10.1016/j.ijmedinf.210210.007

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future direction for behavioral information security research. Computers & Security, 32, 90-101. doi: 10:1016/j.jbi.2010.05.003 Cushman, R., Froomkin, a M., Cava, A., Abril, P., & Goodman, K. W. (2010). Ethical, legal and social issuesfor personal health records and aplications Journal of Biomedical Informatics, 43(5 Suppl), S51-5 doi:10.1016/j.jbi.2010.05.003

Da Veiga, a., & Eloff, J.H.P (2010). A framework and assessment instrument for information security culture. Computers & Security, 20(2), 165-172. Doi: 10.1016/S0167-4048(01)00209-7

Dhillon, G.(2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. Computers & Security, 20(2), 165-172. doi: 10.1016/S0167-4048(01)00209-7

Existing, W., & From, C.(2012). Assesment Of Cobit Maturity Level With Exiting Conditions From Auditor,10(6), 41-50.

Fernandez-Aleman, J. L., Sensor, I.C., Lozoya, P.A.O., & Toval, A.(2013). Security and privacy in electronic helath record; a systematic literature review. Journal of Biomedical Informatics, 46(3), 541=62.doi:1016/j.jbi.2012.12.003

Fernando, J.I., & Dawson, I. I (2009). The health information system security threat lifestyle an

informatics theory. International Journal of Medical informatics, 78(12). S 15-26.doi:10.1016/j.ijmedinf.2009,08.006

Ferralolo,D. F., Sandhu, R., Gavrilla, S., Kuhn. D.R., & Chandramouli, R R. (2001). Proposed NISTstandard for role-based access control. ACM Transactions on information and System Security, 4(3) 324-374. doi: 10.1145/501978.501980

Fielden, K (2010). Information Security Framework. IEEE SECURITY & PRIVACY, 25-30

Fuchs, L.Pernul. G., & Sandhu, R.(2011). Roles in Information security – A survey and classification of the research area. Computers & security, 30(8), 748-769. doi:10.1016/j.cose. 2011.08.002.

Fuchsberger, A. (2005). Intrusion Detection System and Intrusion Prevention Systems. Information Security Technical Report, 10(03), 134-139. doi:10.1016/j.istr.2005.08.001

Furnell,S., & Rajandran, A . (2012). Understanding the influences on information security behavior. Computer Fraud & Security, 2012(3), 12-15,doi: 10.1016/SI361-372(12)70053-2

Ghazvini, A., & Shukur, Z., (2013). Security Challenges and Success Factors of Electronic Healthcare System Procedia Technology, 11(Iceei), 212-219.doi:10.1016/j.protcy.2013.12.183

Guo,K.H.(2012). Security-Related Behavior in Using Information System in the Workplace: A Review and Synthesis. Computers & Security, (1), 1-10. doi:10.1016/j.cose.2012.10.003

Guo,K.H.(2012). Security-Related Behavior in Using Information System in the Workplace: A Review and Synthesis. Computers & Security, 32 (1), 242-251.doi:10.1016/j.cose.2012.10/003

Has, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Muller, G. (2011). Aspects of privacy for electronic health records, International Journal of Medical Informatics, 80(2), e26-31 doi:10.1016/j.ijmedinf.2010.10.001

Hayrinen, K., Saranto, K., & Nykanen, P,(2008). Definition, structure, content, use and impacts of electronic health records: a review of the research literature. International Journal of Medical Informatics, 77(5), 291-304, doi:10.1016/j.ijmedinf.2007.09.001

Huang, L.-C., Chu, H.-C., Lien, C.-Y., Hsiao, C.-H., & Kao,T. (2009). Privacy preservation and information security protection for patients' portable electronic health records Computer in Biology and Medicine, 39(9), 743-50, doi:10.1016/j.compbiomed.2009.06.004

Humaidi, N. (2013). Exploratory Factor Analysis of User's Compliance Behavior towards Health Information System's Security. Journal of Health & Medical Informatics, 04(02), 2-9 doi:10.4172/2157-7420.1000123

Ifineedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. Information and Management, 51(1), 69-79 doi:10.1016/j.im.2013.10.001

Ismail, A., Jamil, A, T., Rahman, A. F. A., Madihah,J., Bakar, A., & Saad, N. M. (2010). Original Article The Implementation of Hospital Information System (His) in Tertiary Hospitals In Malaysia: A Qualitative Study, Malaysian Journal of Public Health Medicine, 10(2), 16-24