International Journal of Applied Sciences: Current and Future Research Trends
(IJASCFRT)
ISSN (Print) , ISSN (Online)

https://ijascfrtjournal.isrra.org/index.php/Applied_Sciences_Journal

Security Control Model for Electronic Health Records

Lucy Kemboi[a]*, LamekRonoh[b]

[a]*Moi University, P.O. Box 3900-30100, Eldoret Kenya*
[b]*Rongo University, P.O. BOX 103 -40404, Rongo, Kenya*
[a]*Email: goinlucy@gmail.com*
[b]*Email: ronohlamek@gmail.com*

Abstract

Secure Electronic Health Records (EHR) is essential in provision of reliable information to support delivery of healthcare services. There is need of a security control model due to the increasing collection of Electronic health records. This study developed a model that will ensure the Electronic Health Records is secure from any threat that will compromise the safety of patient's information at the Moi Teaching and Referral Hospital. This model ensures a proper organized structure for enforcing information security and vital approaches, techniques, procedures and necessary policies and technologies to ensure confidentiality, integrity and availability to ensure a secure EHR.

Keywords: Electronic Health Records; Security Control Model; Information Security.

1. Introduction

Applications and technological solutions to harness risk are not properly used since the ICT capacity in MTRH has grown as demonstrated by implementation of Integrated Hospital Management Information System (I-HMIS) and the improvement of the Local Area Network and Data centre at the Hospital. The hospital faces challenges in information security of the Electronic Health records by virtual attacks as well as potential threats, it encounters information security challenges on, physical, technical and administrative security controls, because of the physical failure of infrastructure, damaged from natural or environmental hazards, and unauthorized access by personnel or external parties. It has also encountered challenges of laptops being stolen, leading to delay in safety of patient's information, inadequate Wi-Fi signals and poor network connectivity [12].

---

* Corresponding author.

2 .Statement of the problem

With the growth of the internet, and with the increase and dependence on computerized systems to support the operations, there has been escalation of security concerns about misuse of information by unauthorized parties, leading to leak in patient information, medical fraud, serious legal implication and financial constrain. To ensure that the information is secure a model that is holistic is required to manage information security.

MTRH lacks a security control model to authenticate security policies that are intended to provide set of rules that the electronic health records system can follow to implement the fundamental security concepts, processes and procedures contained in security policies, these are the processes and methodologies involved with keeping information confidential, available, and assuring its integrity. A Security control model is required to ensure that the security of the electronic health records is well managed.

HIPAA, the Health Insurance Portability and Accountability Act, establishes the standard for protecting patient data including use, storage and transmittal of electronic health information. HIPAA Compliance and breach prevention is required for Protected Health Information (PHI) However; the management of Electronic health records has not received the attention it deserves at the Moi Teaching and Referral Hospital (MTRH) therefore a Security control model is required to ensure that the patient information is protected through the implementation of access control features that will help create and enforce access controls such as passwords, programmed lockouts, health data protection to audit logs for access and data manipulation. This security policies and rules conform to the attribute-based control model. This Supports user authentication, data encryption implementation, User Passwords, access control, Audit trail / log supported analysis of audit trails reports and Automatic logoff should be implemented automated database backup and Data Encryption within the Database [14].

3. Study Objective

To model a security control model for EHR system for MTRH.

4. Literature Review

The standardization develops communication protocol, gadget interfaces, applications and working systems that support standards information exchange. This should conform to the WHO health informatics standards and other international standards among them ISO 9126-1 on software product quality and ISO 27799 on information security management in health on system analysis, design, development, implementation, testing, operation, maintenance and support.

Health information system gathers data from health and other important sectors, investigate the data and ensures their general quality, significance and timeliness, and changes the data into information for health-related decision making. Sound and reliable information is the foundation of decision-making across all health system building blocks. Health information system is also essential for monitoring and evaluation, that also serves as an alert and early warning capability and supports patient and health facility management by enabling planning,

stimulating research, permitting health situations, orienting global reporting and reinforcing communication of health challenges to different users [16].

4.1. Secure Electronic Health Records

Electronic health system is described as the software of facts and communication technologies throughout the complete range of functions that impact on the Personal Health Information (PHI). The EHR serves as the central database where physicians orders for lab x-rays and other lab tests, it enables the hospital and the physicians with the ability to track the information they need to follow the insurance companies and federal regulation [12]. The EHR system has the potential to expand the availability of clinical information and to improve clinical and general health research. However, there are several strategies for assessing information security risks and most of them include identifying dangers and vulnerabilities, examining the likelihood and effect related with the known threats, and ultimately, prioritizing the risks to decide the appropriate level of training and controls necessary for effective mitigation [3].

Security and protection executions are specific, Privacy is handling policy, but security is managing the tools to implement the policy. [13] suggested that private cloud is the cloud infrastructure exclusively for single organization's tasks, whether managed internally outsourced by a third party. Since the business processes that are working on the private cloud could be significant, it is fundamental to provide a protected environment for organizations to execute their activities. As user mobility is a significant component for the present systems, low-cost and adaptable private cloud joining technologies are in strong demand.

The security of EHR systems is a significant aspect in planning, executing and managing the shared care paradigm, the security and protection of EHRs need to be distinguished and defined [8]. As a feature of the IT industry Cloud Computing is making quick progress. Alongside advantages of this innovation credit dangers exist [13]. In the security of health information study, some researches were found with a focus on technological solution to protect the privacy of patients in the wired and remote networks of a medical center [17].

Similar to other organizations, healthcare organizations are in danger of information security threats. Therefore, they are urged to utilize and share electronic health information, making them targets for data breaches due to the value of health information, making it difficult to secure the health information in the healthcare organizations [3].

The most known threats to the information security are unapproved utilization of software and hardware for communications and unlawful activities. The released employees can be another threat to data trustworthiness and to conquer this issue, the users' access level should be confidential.

[10], uncovered that user name and password were the most significant techniques to verify the nurses, and also the huge dimension of information security protection was allocated to administrative and logical controls. There was no significant distinction between opinions of both groups and the levels of information security protection.

Reference [7] states that health information security manages three angles; to be specific, protecting patients' data confidentiality, guaranteeing data integrity, as well as ensuring data availability. Disregarding any of this perspective may cause a various issue, such as legal issues or financial misfortunes for hospitals and health care providers [10]. Improving information security will expand the confidence of patients and clinicians, and may prompt the better utilization of the health data [5]. Therefore, the procedure of risk assessment or risk analysis is the first step in the process of risk management [18].

4.2 Security Control Models.

4.2.1 Bell—LaPadula Confidentiality Model

It is a model that enforces the confidentiality aspects of access model. The model focuses on ensuring that the subjects with different clearances (top secret, secret, confidential) are properly authenticated by having the necessary security clearance, need to know, and formal access approval-before accessing an object that are under different classification levels (top secret, secret, confidential). The rules of this model is a security rule (no read up rule) that states that a subject at a given security level cannot read data that resides at a higher security level.

4.2.2 Clark—Wilson Integrity Model

This model addresses the integrity of information. It separates data into one subject that needs to be highly protected, referred to as a constrained data item (CDI) and another subset that does not require high level of protection, referred to as unconstrained data items (UDI). Its Components are Subjects (users), procedures, software procedures such as read, write, modify that perform the required operation on behalf of the subject (user). Integrity goals of this model is to prevent unauthorized users from making modification without authorization

4.2.3 Harrison—Ruzzo—Ullman Model

This security control model is developed under the rules of the three models above by considering main patient’s information security controls which are administrative, technical, and physical safeguards. The dangers of the EHR are grouped into organizational and systemic threats. Organizational dangers emerge from inappropriate access of patient’s data by either internal or external agents while systemic threats arise from agents in the information flow chain misusing the disclosed data past its planned use. Internal threats can be controlled by an individual or an organization while external threats are those that an individual or organization has no control over [2,15], states that to investigate information security in hospitals, the three main safeguards should be considered.

4.3Technical Security

Technical controls incorporate passwords, firewalls, network intrusion detection systems, and access control lists and data encryption

Its work is to ensure that the information when it is being transmitted through the network, information encryption, and other Internet Transfer Protocols are overseen, in order to limit access to records. Another method of safeguarding electronic patient record is through the use of biometrics (e.g. fingerprint ID recognition) to secure access to computers on networks and information storage devices [4].

4.4 Physical Security

The physical safeguard isn't just utilized in an organization to secure the data integrity, data availability and data confidentiality but also keep protection of physical computer environment system, instruments to be protected from fire and also intrusion. It prefers mostly to utilize the control access to computer system [5].

4.5 Administrative Security

Administrative Procedure is intended to conform to act by the policies and procedures. That sort of administrative procedure is used to maintain the protection of data integrity, data availability and data confidentiality in health care system. Institutions are urged to adopt reasonable and appropriate policies and procedures that comply with the incidences of losses. It is also expressed that majority of the attacks occur after contracts of staff were terminated [1].

5. Methodology

The study adopted a cross sectional survey study design on security of patients' Electronic Health records. The study design enabled an in- depth study of the research objects at a given point and time [6]. This study was carried out at MTRH, Eldoret, Kenya. This is the second largest hospital in Kenya after Kenyatta National Hospital, and is a teaching hospital for Moi University school of Medicine, Nursing, Dentistry and Kenya Medical Training College Eldoret and other health care teaching institutions. The hospital has a 796-bed capacity and serves not only the residents of Uasin-Gishu County but also the residents of the entire western region of Kenya. The population of this region, which includes North and South rift valley, Nyanza and western regions, is estimated to be 15 million people. MTRH also receives patients from Eastern Uganda and Southern Sudan.

MTRH was chosen as the study area because it the second largest referral hospital in the country and the largest hospital in the region and the most equipped hospital with more funding and with more heath records staff compared to other hospitals in the region.

6. Results and discussions

6.1.1 Technical security controls

The study shows that the hospital needs to have smoke and heat sensors in case of fire outbreak and Intrusion and detection system is important to monitor malicious activity within the hospital. The technical security requirements are needed to be put in place to protect patient's information by integrating solution with security

culture and education [9].

6.1.2 Physical Security controls

There is need to have good physical security controls in place to secure patients information. Physical security controls ensure that not only the authorized personnel have access to the facilities that house data so as to secure data integrity, availability and confidentiality but also keep protection of physical computer environment system from fire and intrusion and catastrophic events such as fire and smoke are underlying human threats that are inappropriate to the network. The rooms with patient health information should be fireproof, have installed temperature controls, air conditioning and fire sprinklers. This is advised by [5].

6.1.3 Administrative Security Control

The study showed that most of the administrative security controls are in place in terms of the security procedures and policies, but most of the policies need to be strengthened, since most respondents seem not to know that there are existing procedures and policies that guarantee information confidentiality, availability and integrity. Therefore [10], states that lack of training, lack of instructions for managing security issues and absence of clear and archived policies to deal with the risk factors may raise problems for employees and the organization.

6.2 Model a security control model for EHR system

This study designs a security control model that will ensure a secure EHR for MTRH. The goal of this security control model is to reduce the level of risks to the IT systems and its data at acceptable level. The model should be effective in terms of system compatibility, legislation, regulation, organization policy, safety, reliability and operational impact.

This security control model will enable the results of the risk assessment process that will provide input to the risk mitigation process which is recommended and procedural, so that the technical, physical and administrative controls are evaluated, prioritized and implemented. Therefore, information being an important asset to the hospital**,** it should adequately be protected. Therefore, all the three security controls should take into consideration and equally put in place. The study findings showered that the hospital focuses more on administrative security controls and little is done on the technical and physical security control. Information security improves the patient confidentiality and leads to a secure and easy use of electronic health. Records and technology are completely accountable. Therefore, proper security measures include a good infrastructure, software, hardware, communication and good planning. This will improve information security and expand the confidence of patients and clinicians and prompt better utilization of health data and promote a secure electronic health records system. This security control model is equally represented by the three security controls, the Technical, Physical and Administrative controls. The management, Auditors, Security professionals and all the Hospital members of staff are guided by the Security standards, laws and Regulations, the hospital objectives and the compliance requirements as they go on with their day to day duties at the hospital.

The security standards, laws and regulations, the objectives and compliance drive the three security controls and any threat is detected early enough and the management and the Hospital staff is alerted. This model ensures that the patient information is safe from any unauthorized entity.

6.3 Security Control Model

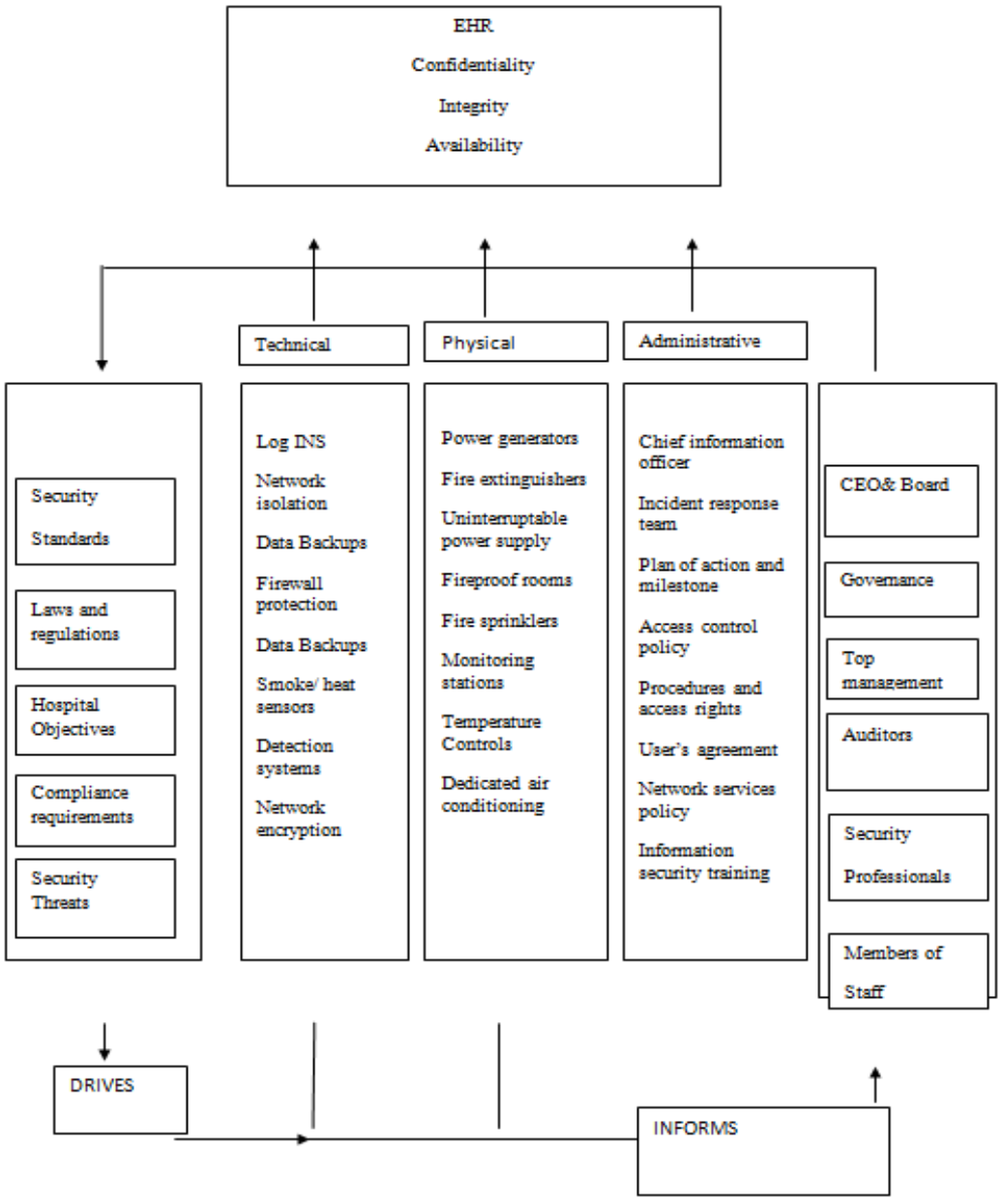

Figure 1: Security Control Model

6.4 limitations

The major limitation of this research was on how to effectively communication the findings of the study to the

management and stakeholders on which formed the strata of this study. More specifically, advising a health facility as to which security technique is appropriate for them to implement was a huge constraint.

Secondly, the cost of individual security technique or measure to have been recommended to a facility was not captured in this study.

Furthermore, the major constraint of this study was failure to study ICT security for each facility exhaustively so as to give salient features unique to each health facility as far as patient's security records are concerned.

6.5 conclusion

The study also concludes that there is need to establish security controls for EHR in MTRH since new technologies in place, the hospital management should train staff on the risks, threats, policies and guidelines that will greatly increase information confidentiality, availability and integrity making the electronic health records system more secure.

The results also indicate that most of the administrative security controls are place and contributes more to information security, these include; procedures and policies. Most of the health records staff agreed on the information security policies and procedures, they seem to agree that they are in place and working. Unlike the administrative security control, most of the staff disagreed on the technical and physical security control in MTRH

6.6Recommendation of the study

The researcher recommends a model that will ensures a secure electronic health records system whose outcomes serves as a desired output to protect the information properties of confidentiality, integrity and availability. This is represented by the three security controls in equal measures, Technical, physical and administrative controls. This model shows that as the CEO, top management, auditors and all hospital members of staff do their duties in the hospital, are guided by security standards, laws and regulations, hospital objectives and all the compliance requirements. As a result, they are bound to come across security threats, these threats will be intercepted by the three security controls which will inform the hospital management, auditors and all the parties involved.

This security control model will be implemented when all the three security controls are in place, with the technical, physical and administrative security controls, the INFOSEC triad- confidentiality, integrity and availability interchangeably contributes to goals of and fundamental aspects of the building block in information security. The figure below presents the security control model.

References

[1]. A.Appari and M. Johnson, "Information security and privacy in healthcare: current state of research", *International Journal of Internet and Enterprise Management*, vol. 6, no. 4, p. 279, 2010. Available: 10.1504/ijiem.2010.035624.

[2]. C.Kruse, B. Smith, H. Vanderlinden and A. Nealand, "Security Techniques for the Electronic Health Records", *Journal of Medical Systems*, vol. 41, no. 8, 2017. Available: 10.1007/s10916-017-0778-4.

[3]. E. Mehraeen, H. Ayatollahi and M. Ahmadi, "Health Information Security in Hospitals: the Application of Security Safeguards", *Acta Informatica Medica*, vol. 24, no. 1, p. 47, 2016. Available: 10.5455/aim.2016.24.47-50.

[4]. E. Söderström, R. Åhlfeldt and N. Eriksson, "Standards for information security and processes in healthcare", *Journal of Systems and Information Technology*, vol. 11, no. 3, pp. 295-308, 2009. Available: 10.1108/13287260910983650.

[5]. H.Ayatollahi and G. Shagerdi, "Information Security Risk Assessment in Hospitals", *The Open Medical Informatics Journal*, vol. 11, no. 1, pp. 37-43, 2017. Available: 10.2174/1874431101711010037.

[6]. J. Winterton, "Review: Business Research Methods ALAN BRYMAN and EMMA BELL. Oxford: Oxford University Press, 2007. xxxii + 786 pp. £34.99 (pbk). ISBN 9780199284986", *Management Learning*, vol. 39, no. 5, pp. 628-632, 2008. Available: 10.1177/1350507608090050804.

[7]. J. Zarei and F. Sadoughi, "Information security risk management for computerized health information systems in hospitals: a case study of Iran", *Risk Management and Healthcare Policy*, p. 75, 2016. Available: 10.2147/rmhp.s99908.

[8]. J.Fernández-Alemán, I. Señor, P. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review", *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541-562, 2013. Available: 10.1016/j.jbi.2012.12.003.

[9]. J.Kwon and M. Johnson, "Security practices and regulatory compliance in the healthcare industry", *Journal of the American Medical Informatics Association*, vol. 20, no. 1, pp. 44-51, 2012. Available: 10.1136/amiajnl-2012-000906. .

[10]. M. Samadbeik, Z. Gorzin, M. Khoshkam and M. Roudbari, "Managing the Security of Nursing Data in the Electronic Health Record", *Acta Informatica Medica*, vol. 23, no. 1, p. 39, 2015. Available: 10.5455/aim.2015.23.39-43.

[11]. M.Bakhshi, H. Monem, O. Barati, R. Sharifian and M. Nematollahi, "Structural investigation of websites of selected educational hospitals of Shiraz University of Medical Sciences from Patient Relationship Management (PRM) perspective", *Electronic Physician*, vol. 9, no. 7, pp. 4786-4790, 2017. Available: 10.19082/4786.

[12]. N. Muinga et al., "Implementing an Open Source Electronic Health Record System in Kenyan Health Care Facilities: Case Study", *JMIR Medical Informatics*, vol. 6, no. 2, p. e22, 2018. Available: 10.2196/medinform.8403.

[13]. Reaching for the Cloud(s): Privacy Issues related to Cloud Computing - March 2010 - Office of the Privacy Commissioner of Canada", *Priv.gc.ca*, 2021. [Online]. Available: https://priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2010/cc_201003/. [Accessed: 09- Nov- 2021].

[14]. S.Chukkapalli et al., "Ontologies and Artificial Intelligence Systems for the Cooperative Smart Farming Ecosystem", *IEEE Access*, vol. 8, pp. 164045-164064, 2020. Available: 10.1109/access.2020.3022763.

[15]. Strategic information systems: concepts, methodologies, tools, and applications", *Choice Reviews*

Online, vol. 47, no. 08, pp. 47-4186-47-4186, 2010. Available: 10.5860/choice.47-4186.

[16]. *Who.int*,2021.[Online].Available:https://www.who.int/healthinfo/systems/WHO_MBHSS_2010_section1_web.pdf. [Accessed:09- Nov- 2021].

[17]. Y. Alotaibi and F. Federico, "The impact of health information technology on patient safety", *Saudi Medical Journal*, vol. 38, no. 12, pp. 1173-1180, 2017. Available: 10.15537/smj.2017.12.20631.

[18]. Y.Al-Issa, M. Ottom and A. Tamrawi, "eHealth Cloud Security Challenges: A Survey", *Journal of Healthcare Engineering*, vol. 2019, pp. 1-15, 2019. Available: 10.1155/2019/7516035.