ISSN No:-2456-2165

Security Control Requirements for Electronic Health Records

Lucy Kemboi[1]
Rongo University
MSC Health Informatics Student

James Abila[2]
Rongo University
Lecturer, Department of Informatics and Information Science

Lamek Ronoh [3]
Rongo Univerist
Lecturer, Department of Informatics and Information Science

Abstract:- Health Information System is fundamental in provision of dependable information in support of delivery of healthcare services. The adoption of Electronic Health Records (EHR) provides improved patient care and a more efficient practice management. However the use of EHR raises concerns over protection of patient's information in terms of security of patient's information. This study established security control requirements for electronic health records to 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. The investigation embraced an arbitrary testing system to choose an example of 97 out of 133 health records members of staff and and questionnaires designed for data collection. The information gathered from the research instrument was coded and examined utilizing Statistical Package for Social Sciences (SPSS) adaptation 22.0.

Keywords:- *Electronic Health Records, Information Security, Security Controls.*

I. INTRODUCTION

[18] Defined a health system as the whole being equal, associations, and resources administration, great assistance conveyance and access to basic medication. A good health system requires a vigorous financing component, a well-prepared and adequately paid workforce, dependable information system, good leadership and governance, good service delivery and access to essential medicine.

Globally, Denmark is viewed as "a main nation in eHealth integration and healthcare services delivery" [9]. It is also viewed as a world chief in eHealth adoption with secure intranets setup to link areas with local health authorities and other associations. This has been cultivated through virtual private network (VPN) connections to create an Internet based healthcare data network. Electronic health records are utilized by practically all broad practitioners in Denmark at 100% penetration, roughly, 74% by full time experts and all drug store.

Regionally, in Zambia Smart-care was Smart-care was made to address the issues of the Ministry of Health in taking care of by HIV patients, thinking of the element of the foundation and advancement in the health sector in Zambia [13]. In 2006, after two years of powerful pilot tests, smart-care was supported as "the sole electronic medical record to be used for public and private health care in Zambia". The main reason of the smart-care program was to interface up services for HIV clients and improve access to health information regardless of area, subsequently, limiting delays in the beginning of treatment, duplication of examinations, dangers and mistakes, costs and improving HIV data standards, security and confidentiality in the country [14].

Locally, the Kenyan government, working with all inclusive partners and local organizations, "built up an eHealth strategy, with standards, and rules for electronic health record appropriation in public hospitals and executed two major health information technology ventures" District Health Information Software Version 2, for examining national health care indicators and a rollout of the KenyaEMR and International Quality Care Health Management Information Systems, for foreseeing 600 HIV clinics aall over the country.

➢ *Statement of the Problem*

Health information is potentially very sensitive and should not be accessible by persons who have no need or authorization for that information. Security plays a large role in medical information. The "Kenya Health sector referral implementation guidelines" supports advances of linkages across the different stages of care between public and private hospitals to improve the health system's capacity to move clients, client parameters, specimens and expertise between the different stages of the health care system from the national health referral Services (level 6) to county referral hospital (level 4 and 5)". With the growth of the internet, and with the increase and dependence on computerized systems to support the words operations, there has been escalation of security concerns about misuse of information by unauthorized parties. Majority of the information security failure occurs because of violations of controls by trusted personnel. To ensure that the information is secure a model that is holistic is required to manage information security. Moi Teaching and referral hospital(MTRH) lacks a security control requirements that authenticate security policies that provide rules that the electronic health records system can follow to implement the concepts, processes and procedures contained in security policies, as referred by INFOSEC (Information security), these are the processes and methodologies that contains keeping information private, accessible, and guaranteeing its integrity. They prevent unauthorized personnel from entering or accessing a system. Security control requirements will quarantee that the security of the

electronic health records is well all round and adequately assured of the administrative controls and incorporates technical security controls and physical controls.

- *Study Objective*

To establish security control requirements for EHR in MTRH.

- *Research Question*

Which are the security control requirements for EHR in MTRH?

II. LITERATURE REVIEW

A. Introduction

The standardization will create correspondence convention, device interfaces, applications and working systems that will support standard information exchange. This ought to adjust to the WHO health informatics standards and other worldwide principles among them ISO 9126-1 on programming item quality and ISO 27799 on information security board in health on system analysis, structure, improvement, execution, testing, activity, upkeep and support. The possibility of information security has been institutionalized and characterized by WHO health informatics benchmarks and other global measures including, ISO, all the more expressly by the standard ISO/IEC 27799 on data security the board and ISO 9126-1 on programming quality. "The standard gives rules for information security board and defines the security in three terms; Secrecy, Accuracy and Accessibility. Secrecy manages the possibility that information should just be open to those with right approval to peruse and use the information.

B. Secure Electronic Health Record

The Electronic Health Record (EHR) is described as digitally stored information about a person's lifetime to help progression of care, education and research and and guaranteeing classification consistently and the IT foundation that permits sharing of restorative information. [11] Electronic health system portrays the software of realities and correspondence technologies all through the total scope of capacity that affect the Personal Health Information (PHI).

The EPR will strengthen the situation of the patient since they will have more and easier control over their health information and can pursue the advancement of their own sicknesses. Electronic Patient Record frameworks (EPRS) reason is to offer a domain that is secure [5].

The EHR system can possibly grow the accessibility of clinical data and to improve clinical and general health research". "Anyway there are a few techniques for evaluating information security dangers and the greater part of them incorporate recognizing risks and vulnerabilities, inspecting the probability and impact related with the known dangers, and eventually, organizing the dangers to choose the suitable degree of preparing and controls important for successful mitigation [7].Information Security issues in Germany was arranged into (hierarchical shortcomings, human blunder, specialized disappointment and purposeful acts). "Control measures were foundation, association, staff, programming and equipment, correspondence and possibility arranging". [3] "Current culprits are concentrating on most important corporate and legislative information and misusing vulnerabilities without security and laxity in security issues inside the association [17]. [7] Found that "a greater amount of information ruptured in the year 2013 influenced 43.8% of healthcare organizations' contrast to 34% of the business associations". [3] Outcomes demonstrated that among the "a data security danger, fire was seen as the highest hazard factor". "Human and physical dangers were among the low probability element". Concerning the information security controls used in the healthcare, the results showered that the "use of the technical controls were the most regular (91.7%) differentiation to the administrative (87.5%) and the physical controls (66.7%)". [6] Detailed that "in the year 2013, health records for 68 patients were lost when a nurse of a Hong Kong hospital lost a USB drive with individual treatment information including the national social security numbers for patients". [8] Suggested that the requirements for "research and development of an effective information security is to guarantee that the patient's information is protected in Kenyan hospitals which will ensure accountability in handling patient's information". In this research, "we built up an EHR system security control requirements that will be utilized to enhance the security of the EHR on an insignificant spending plan in public referral hospitals". [19] In Iran showered that various studies had been directed about the information security in healthcare and a couple of them focused on "evaluating health information security dangers as key elements and fundamental reasons for them. In Africa, [1] understood, that the executions of EHR system every now and then relied upon international aid, making maintainability, security and improvement troublesome and furthermore with dread that both the doctor and patient might be presented to the world using the web.[8], suggested the need for research and development of an effective information security model to ensure the protection of patients 'information in Kenyan hospitals which will ensure accountability in handling patients' information. In this investigation, review the security control requirements that will be used to improve the security of the EHR system at MTRH. This literature review concentrated on how information security will guarantee a protected EHR. Access control should be implemented for users of the EHR system. Screen savers and time-out breaks should be implemented on the system just in-case a user forgets to logout. Passwords should be changed periodically in the case where staff members are transferred or dismissed [12]. The three main patient's information security controls requirements are administrative, technical, and physical controls [16]. Dangers to security of EHR are grouped into Organizational dangers that emerge from misuse of access of patient's data by either internal or external agents and systemic threats that arise from agents in the information flow chain misusing the disclosed data past its planned use [4]. 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. To investigate information security in hospitals, three main security controls should be taken into account [15].

➢ *Technical Security*

Technical controls "manages access to computer system information and ensure interchanges when information is being transmitted over several networks electronically". Additionally, "it has to protect the data integrity, data confidentiality and availability but the mainly it protects, controls and monitors the information access". "Technical controls contain use of passwords, firewalls, network intrusion detection systems, and access control lists and data encryption".

➢ *Physical Security*

Physical security controls accesses the computer systems and Facility access controls. Requirements of physical controls include "locks and alarms", that ensures only authorized personnel have access into the. Facilities that house systems and data, these workstation security measures, such as cable locks and computer monitor privacy filters guard against theft and restrict access to authorized users". "The security standards under physical controls include facility access controls, workstation use, workstation security, and device and media controls".

➢ *Administrative Security*

Administrative controls are intended to conform to the policies and procedures. "These administrative controls are used to maintain the protection of data integrity, data availability and data confidentiality in health care system". Institutions are encouraged to adopt reasonable and appropriate policies and procedures that comply with the incidences in the case of losses [2].

III. METHODOLOGY

➢ *Introduction*

Descriptive survey was conducted using 200 respondents in eight Health Records departments across the Moi Teaching and referral hospital in Eldoret- Kenya. This study was carried out at MTRH, Eldoret, Kenya. The instrument used to collect the data was questionnaire**.** To ensure the reliability of the questionnaires, a pilot study was carried out first before administering all the research questionnaires. Reliability and validity coefficient of 0.70 or 70% and above was considered acceptable.

IV. RESULTS AND DISCUSSIONS

❖ *EHR Security Controls Requirements*

This security requirement for securing EHR in MTRH contains technical, physical and administrative security controls that must be put in place to ensure that the patient's information is secure. The analysis showered that the EHR system in MTRH is at risk and that all the three security controls should contribute equally to information security**.**

➢ *Technical Security Controls*

The respondents were positive that the hospital ensures that the health records data is backed up regularly at 60.8% and that the user rights were reviewed frequently at 70.1%. 71.1% disagreed that the smoke sensors and heat sensors were in place.55.7% disagreed that intrusion detection systems software application and devices were in place to monitor any malicious activities. 54.6% disagreed that the hospital has ensured that there are Log- INS and access to particular applications to prevent any unauthorized user. 60.8% disagreed that firewall is installed to block any unauthorized activity within the system. 44.3% agreed that the hospital network has been encrypted so that unauthorized users don't understand the information. 53.6% of the respondents disagree that the network being used by the staff handling patient health records is isolated from the network being used by members of staff not handling patient's records. Technical Security control requirements is to protect data integrity, confidentiality and monitor information being transmitted through the network and is encrypted in order to limit access, and also secure access to computers on the network and information storage devices [2]. Technical controls also help in detecting and mitigating information risks [16].

This depicts that the technical security requirements are partially in place. They should be installed in the hospital to protect patient's information by integrating solution with security culture and education. [10].

➢ *Physical Security Controls*

The respondents strongly agreed at 93.9% that the generators had been installed in the hospital to be used in case the electricity goes out. 74.2% disagreed that fire sprinklers were installed at the health records section to put out fire in case fire breaks out. 41.2% strongly agreed that fire extinguishers are installed in case of fire. 68.0% disagreed that the uninterruptable power supply were installed at the health records section. 68% of the respondents disagreed that rooms with patient information are fireproof and not secure while 63.9% disagree that Temperature controls and air conditioning are place, and.51.5% disagree, that there is a monitoring station at the hospital to monitor the daily occurrence. [3] states that physical controls ensures that only authorized personnel have access to the facilities that house data therefore promoting integrity, availability and confidentiality and also to 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.

Therefore these study advices on good physical security controls to be installed in place to secure patients information.

➢ *Administrative Security Control*

The respondents were very positive on administrative security controls. 40.2% strongly agreed that the reports are reviewed regularly by the Chief Information Security Officer. 47.4% agreed that there is a computer incident

response team in place in case of the system failure. , disagree, 34.0% agree and 26.8% were uncertain that the hospital has developed a plan of action and milestones for a continuous monitoring, identifying and addressing the systems weakness in security implementation, 44.3% disagreed that the hospital management has developed and published a written access control policy on information security, The respondents further agreed that there are procedures for removing access rights for a terminated employee, at 64.9%. The respondents further agreed at 75.3% that the hospital has written procedures for creation and deletion of user accounts. 60.8% agreed that users are required to sign access agreement. Default passwords for the system devices or application are allowed anywhere in the hospital 52.6% disagreed. There is a developed and written policy on the use of network services within the hospital 45.4% disagree. 69.1% of the respondents agreed that when a new account is created, the user is required to change to his/her password conforming to the hospital policy.

[7], 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. This shows that the administrative security controls contributes more to the security of EHR system compared to the technical and physical controls.

V. CONCLUSION

This research was conducted at MTRH which is the second largest referral hospital in Kenya, serving the people from the Rift valley, western and Nyanza Regions. This study established the security control requirements for EHR in MRTH. The three security controls were analyzed separately and therefore demonstrated that the three security controls did not equally contribute to the information security of the Electronic Health Records in MTRH. It shows that the administrative security controls contributes more to the security of EHR more than the Technical and Physical security controls.

RECOMMENDATION

This study recommends that the users be trained regularly so that there are minimal mistakes when handling the system, and that they understand more on what the controls entails. The users should also be trained in backing up of information to avoid losing patients information. The hospital should ensure that the user rights reviewed frequently to eliminate those who have no authorization to access patient records, smoke and heat sensors should be installed as an alert incase of fire. The hospital should ensure that there an Intrusion Detection software application is in place to monitor computer systems for any malicious activity and violation. There should be system and monitoring tools used to record log -INS and access to particular application to prevent unauthorized users. The firewall should be installed to block any unauthorized activity within the system. The network being used by the health record staff should be isolated from the network being used by other staff members not handling patient's records. Fire sprinklers should be installed at the health records departments to suppress fire in case of fire break out. Uninterruptable power supply should be installed for power backup in case the power goes out. There should be a monitoring station within the hospital to monitor the daily occurrences. Temperature controls and dedicated air conditioning should be installed to cool to cool the equipments incase of excess heat. The hospital should develop a plan of action and milestones for a continuous monitoring, identifying and addressing the system weakness in the security control implementation. The hospital management should develop and publish a written access control policy on information security, curbing security threats within the system. There should be a written policy on the use of network services within the hospital so that there is control of access to the system within the hospital.

REFERENCES

[1]. Akanbi, M. O., Ocheke, A. N., Agaba, P. A., Daniyam, C. A., Agaba, E. I., Okeke, E. N., & Ukoli, C. O. (2012). Use of electronic health records in sub-Saharan Africa: progress and challenges. *Journal of Medicine in the Tropics*, *14*(1), 1.

[2]. 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), 279-314.

[3]. Ayatollahi, H., & Shagerdi, G. (2017). Information security risk assessment in hospitals. *The open medical informatics journal*, *11*, 37.

[4]. Bidgoli, H. (2006). *Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations* (Vol. 2). John Wiley & Sons.

[5]. Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Security requirements and solutions in electronic health records: lessons learned from a comparative study. *Journal of medical systems*, *34*(4), 629-642.

[6]. Gao, X., Xu, J., Sorwar, G., & Croll, P. (2013). Implementation of E-health record systems and E-medical record systems in China. *The International Technology Management Review*, *3*(2), 127-139.

[7]. Hartwig, R. P., & Wilkinson, C. (2015). Cyber Risk: Threat and Opportunity. *Insurance Information Institute*, 2.

[8]. Juma, K., Nahason, M., Apollo, W., Gregory, W., & Patrick, O. (2012). Current status of e-health in Kenya and emerging global research trends 1.

[9]. Kierkegaard, P. (2013). eHealth in Denmark: a case study. *Journal of medical systems*, *37*(6), 9991.

[10]. Kwon, J., & Johnson, M. E. (2012). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*, *20*(1), 44-51.

[11]. Mišić, J., & Mišić, V. B. (2007). Implementation of security policy for clinical information systems over wireless sensor networks. *Ad Hoc Networks*, *5*(1), 134-144.

[12]. Mugo, D. M., & Nzuki, D. (2014). Determinants of electronic health in developing countries.
[13]. Mweebo, K. (2014). Security of electronic health records in a resource limited setting: The case of smart-care electronic health record in Zambia.
[14]. Neame, R. (2013). Effective sharing of health records, maintaining privacy: a practical schema. *Online journal of public health informatics*, *5*(2), 217.
[15]. Ray, A., & Newell, S. (2010). Exploring information security risks in healthcare systems. In *Health Information Systems: Concepts, Methodologies, Tools, and Applications* (pp. 1713-1719). IGI Global.
[16]. Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International journal of multimedia and ubiquitous engineering*, *2*(2), 17-32.
[17]. Sood, S. P., Nwabueze, S. N., Mbarika, V. W., Prakash, N., Chatterjee, S., Ray, P., & Mishra, S. (2008, January). Electronic medical records: A review comparing the challenges in developed and developing countries. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (pp. 248-248). IEEE.
[18]. World Health Organization. (2010). *monitoring the building blocks of health systems: a handbook of indicators and their measurement strategies*. World Health Organization.
[19]. Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk management and the healthcare policy.*