Effectiveness Of Security Controls On Electronic Health Records

Everleen Wanyonyi, Anthony Rodrigues, Silvance Abeka, Solomon Ogara

ABSTRACT: Electronic Health Record (EHR) systems enhance efficiency and effectiveness in handling patients' information in healthcare. This study focused on the EHR security by initially establishing the nature of threats affecting the system and reviewing the implemented security safeguards. The study was done at a referral hospital (level 6) government facility in Kenya. Purposive sampling was used to select a sample of 196 out of 385 staff and a questionnaire designed for qualitative data collection. Data was analyzed using SPSS software. Correlations and binary logistic regression were obtained. Binary Logistic Regression (BLR) was used to establish the effect of the safeguards (predictors) on EHR security. It was established that physical security contributes more to the security of an information system than administrative controls and technical controls in that order. BLR helped in predicting effective safeguards to control EHR security threats in limited resourced public health facilities.

Keywords: electronic health records, cyber security, safeguards, binary logit function

1. Introduction

A productive nation is identified by the health of its people. In turn, people's health is determined by how efficient the health facilities are in terms of service delivery. Patients' health records need to be handled with care for they constitute a treatment trail. Prior to the introduction of Electronic Health Record (EHR) system, patients' records were filed and stored in a specified store with a record management clerk in charge. The paper based records were prone to errors made by illegible handwritings and were sometimes ineffective when used in prescriptions. Paper based records were easily lost since a single patients' record was fragmented across departments. Tracing a patients' information was difficult, the clerk had to manually go through several files to extract the required information. Electronic health records brought about easy storage and access since the records were standardized with no illegible handwritings. Despite the advantages, the EHR system brought a dimension of insecurity whereby malicious people are able to access patients' information in digital form. To secure the EHR system, several safeguards have to be put in place. Financial constraints in public health facilities inhibit the implementation of all safeguards and therefore, a model has to be developed that may guide implementation of these security safeguards with budget limitations in mind. The healthcare sector in Kenya comprises the public system with major players including the Ministry of Health (MoH) and parastatal organizations, the private sector which includes private for profit, Non-Governmental Organizations (NGOs), Faith Based Organizations (FBO) facilities and the local government authorities. The public-sector accounts for 51% of the health facilities [15]. The public healthcare is organized into different levels forming a pyramid-like pattern. At the apex are level 6 hospitals also referred to as tertiary or national hospitals. These hospitals act as referral hospitals for all other hospitals under them.

- *Everleen Wanyonyi, Anthony Rodrigues, Silvance Abeka, Solomon Ogara*
- *School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology*
  E-mails: nekesa2011@gmail.com; tonyr@jooust.ac.ke; sabeka@jooust.ac.ke; sogara@jooust.ac.ke

They serve an enormous number of clients and have implemented the EHR systems for management of patients' and administrative information. In this group is Kenyatta National Hospital in Nairobi, Moi Teaching and Referral Hospital in Eldoret and Jaramogi Oginga Odinga Teaching and Referral Hospital (JOOTRH) in Kisumu. In this paper, we determine the probability of EHR security risk when different ratios of administrative, physical and technical controls are implemented with the help of a binary logistic regression. With the limited resources available in public health institutions, it is practical to determine what to put in place to achieve security of the EHR system without implementing too many security safeguards which may prove to be quite costly. This study will be of benefit to the Ministry of Health (MoH) to access readily available clean data for decision making. The model will strengthen doctor-patient relationship because of confidentiality and privacy assurance. Medical insurers are also to benefit from the model since medical fraud will drastically reduce thus lowering costs. The binary logit regression will help to sample important security safeguards to secure the EHR system with minimal implementation costs.

2.0 Literature

2.1. Background of the Study

Cyber security risks pose serious economic and national security challenges in the 21st century. Cyber security is equated to weapons of mass destruction and jihad since its damages are real with actors stealing, changing or destroying information. Sophisticated criminals are targeting most valuable corporate and governmental information assets by exploiting vulnerabilities in the systems and taking advantage of lack of security and laxity in security issues within the organization [24]. [10] found that majority of data breaches in the year 2013 affected 43.8% of medical/healthcare organizations compared to 34% of the business sector organizations. In Hong Kong, [8] report 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 personal treatment information including the social security numbers for patients. In Africa, [3] realized that the implementation of EHR systems often rely on international aid making sustainability, security and improvement difficult. There is fear that both the physician and patient may be exposed to the world through the use of the Internet [16]. [12] recommend the need for research and development of an effective information security

model to protect patients' information in Kenyan hospitals which will mitigate lack of accountability in handling patients' information. In this study, we develop an EHR system security model that will be used to enhance the security of the EHR on a minimal budget in public referral hospitals.

2.2 Health information security

Information security can be defined as having the right information, provided to the right person, in the right time and at the right place. The patient record Act (SFS 1985:562) of Sweden emphasizes the need to guarantee the security and privacy of patients' records [2]. The United Nations (UN) encourages countries to legislate for EHR protection and to ensure patients are protected after disclosing their health information. By enacting the Data Protection Directive in 1995, the UN was to ensure that patients' information is used within their countries of collection and patients' privacy guaranteed [1]. In Europe, the Data Protection Act, 1998 (DPA) was passed to ensure that EHR information is protected against unauthorized loss or damage by appropriate technical and organizational measures. Access control should be implemented for users of the EHR system. Screen savers and time-out periods should be implemented on the system just in-case a user forgets for example to logout [21]. [11] outlines four controls for patients' information security: administrative controls, physical safeguards, organizational standards and technical safeguards. Institutions are encouraged to adopt reasonable and appropriate policies and procedures that comply with the enforcement of these controls.

2.3 Security threats in EHR

[18], while investigating current information security, privacy and accountability issues in EHR, noted that insider attacks and lack of access control mechanisms have largely contributed to security threats in EHR. Staffs with legitimate access rights commit fraud and sabotage IT infrastructure making it difficult to achieve security. In a study of establishing the challenges for protecting the privacy of EHR, [22] realized that 90% of attackers were insider attacks with high level administrative rights while 81% of attacks involved incidences of losses. It was also established that the majority of attacks occurred after contracts of staff were terminated. [4] classify threats to security of EHR into organizational and systemic threats. Organizational threats arise from inappropriate access of patients' data by either internal or external agents while systemic threats arise from agents in the information flow chain exploiting the disclosed data beyond its intended use. [5] classifies threats to EHR into internal and external threats. 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. EHR security threats in Asia are classified into: common threats, information user threats, business process/application threats and infrastructure threats. Common threats are threats such as viruses and phishing, information user threats include incorrect handling of information due to lack of awareness and external attacks targeting information such as hacking. Business process/application threats occur in the form of interruptions of business processes which hinders availability of the system while infrastructure threats emanate from inside and outside the organization such as denial of service attacks, phishing and social engineering [7]. [13] identify four unique threats to information security in the African continent. First, is lack of cyber security awareness, legislation, policies, and technical cyber security measures. Second, lack of a proper integrated legal framework and policy is a major threat to cyber security. There is need for proper and relevant laws, policies and practices to curb cybercrime. Another cybercrime threat listed is lack of security awareness regulations. Almost 80% of the population in Africa lack basic computer security knowledge and this makes it difficult to control cybercrime. Lastly, lack of technical security measures is also a major threat to cyber security. Users do not have technical security abilities to control cybercrime. [23], indicate that a major threat to EHR system in Africa is single point of failure both in staffing and equipment. Lack of testing, unstable power supplies and lack of technical support are also major threats and risks to the EHR system. Apart from security and privacy issues, developing countries also bear greater burdens due to lack of infrastructure, legislation, EHR policies, training and resources. Kenya faces the same challenges and threats that face other African countries. [16] state that with the introduction of EHR in Kenyan health facilities, there is need for security and privacy of patients' information since the systems are centered on HIV/AIDS. Lack of proper legislation will result in perpetrators going scot free and waning patients' confidence in the system. A case of medical insurance fraud using EHR was reported in [6] online. The report indicated that fraudsters targeted prominent Kenyans' medical insurance covers to make false medical claims. A former pharmacist at MP Shah and Aga Khan Hospital in Nairobi compiled a list of names of insured persons and used their details to create fake medical cards which bore the names of his fraudsters. These cards were then used to impersonate the bone fide clients and to collect expensive drugs from large hospitals based on prescriptions made by the pharmacist on fake sheets bearing hospital letter heads. The report indicates that in the year 2014, approximately US$ 19 million was paid to fake medical claim fraudsters. Effective implementation of security controls can help in alleviating such security threats to the EHR system.

2.4 Information Security Controls

2.4.1 Administrative

These are also called procedural or management controls. According to [20], administrative controls consist of approved written policies, procedures, standards and guidelines. Administrative controls inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations from the government, corporate policy, hiring policy, password policy and disciplinary policy are administrative controls. Administrative controls are divided into preventive, detective and recovery security controls. Preventive administrative controls assign security responsibility to ensure that adequate security is provided for the mission critical IT systems. They include separation of duties, least privilege and user computer access registration and termination. Conducting security awareness and technical training to end users and system users helps in protecting the organizational mission. Detective administrative controls deal with implementation of personnel security controls including personnel clearance, background investigations, rotation of duties, conducting periodic review

of security controls, performing periodic system audits, conducting risk management to assess and mitigate risks and finally to authorize IT systems to address and accept residual risks. Recovery administrative security controls provide continuity of support and develop, test, and maintain the continuity of operations plan to provide for business resumption and ensure continuity of operations during emergencies or disasters. They establish an incident response capability to prepare for, recognize, report, and respond to the incident and return the IT system to full operational status.

2.4.2 Logical/technical

Logical controls are also known as technical controls. These controls use software and data to monitor and control access to information and computing systems. Examples of technical controls include passwords, firewalls, network intrusion detection systems, access control lists and data encryption. The principle of least privileges is a technical control that requires an individual, program or system process not to be granted any more access privileges than are necessary to perform the task. [17] categorizes technical controls into support, prevent, detect and recover. Supporting technical controls include identification, cryptographic key management, security administration and system protections. Identification control provides the ability to uniquely identify users, processes and information resources. Cryptographic key management includes key generation, distribution, storage and maintenance. Security administration deals with security features of an IT system that must be configured to meet the needs of a specific installation and to account for changes in the operation environment. Finally, system protection represents the quality of the implementation from the perspective both of the design processes used and of the manner in which the implementation was accomplished. Examples of system protection are residual information protection, least privilege, process separation, modularity, layering and minimization of what needs to be trusted. Preventive technical controls inhibit attempts to violate the security policy. These controls include authentication, authorization, access control enforcement, non-repudiation, protection communications and transaction privacy. Authentication provides means of verifying the identity of a subject to ensure the claimed identity is valid. Authentication mechanisms include passwords, PINs, and digital certificates. Authorization control enables specification and subsequent management of the allowed actions for a given system. Access control enforces data integrity and confidentiality. Non-repudiation ensures that senders cannot deny sending information and that receivers cannot deny receiving it. Non-repudiation is applied at the point of transmission or reception. Protected communication ensures the integrity, availability and confidentiality of sensitive and critical information while it is in transit. Protected communication uses data encryption methods like VPN and IPSEC to minimize network threats such as replay, interception, packet sniffing and eavesdropping. Detection and recovery technical controls, according to [17], warn of violations or attempted violations of security policy. They include audit trails, intrusion detection methods and checksums. They are needed as a compliment to the supporting and preventive technical measures because none of these measures is perfect. More detection and recovery controls include proof of wholeness; restore secure state and virus detection and eradication.

2.4.3 Physical

These controls monitor and control the environment of the workplace and computing facilities and they also monitor and control access to and from such facilities. Examples of physical information security controls within the organization include; door and locks, heating and air conditioning, smoke and fire alarms, and suppression systems and fencing. Separating network and workplace into functional areas are also physical controls. It ensures that an individual cannot complete a critical task by himself. An example is a programmer should not be the system administrator at the same time. The roles and responsibilities should be separated from one another so that one person does not start and end a task. Preventive Operational Controls include: control data media access and disposal e.g., physical access control; limit external data distribution e.g., use of labeling, control software viruses; safeguard computing facility e.g., security guards, site procedures for visitors, electronic badge system, biometrics access control, management and distribution of locks and keys, barriers and fences; secure wiring closets that house hubs and cables; provide backup capability e.g., procedures for regular data and system backups**,** archive logs that save all database changes to be used in various recovery scenarios; establish off-site storage procedures and security; protect laptops, personal computers (PC) and workstations; protect IT assets from fire damage e.g., requirements and procedures for the use of fire extinguishers, tarpaulins, dry sprinkler systems; fire suppression system and provide emergency power source e.g., requirements for uninterruptible power supplies, on-site power generators, control the humidity and temperature of the computing facility e.g., operation of air conditioners, heat dispersal. Detection Operational Controls include providing physical security e.g., use of motion detectors, closed-circuit television monitoring, sensors and alarms and ensuring environmental security e.g., use of smoke and fire detectors, sensors and alarms.

3. EHR security moderating factors

3.1 Organizational culture

Organizational culture can be defined as a set of shared values, beliefs, assumptions and practices that shape and direct members attitude and behavior in the organizations. This involves mission statements, values, technologies, practices, etc. What the organization outlines pertaining to information security is what defines the security of information of that organization. If users are trained regularly not to share computer resources, passwords and to properly implement security policies, the security of information will be guaranteed. Organizational culture is the single most important factor accounting for success or failure of an organization. Since organizational culture would certainly influence the operation activities of an enterprise and the effectiveness of an enterprises information security practice, the managers should regard organizational culture as an important factor for supporting and guiding information security management practice. While information security concerns face each organization, engaging security practices in the organization culture proactively could positively affect

the success of the organization. The most pressing problems on information technology security are caused by negligence of people rather than attack of events, therefore, it is important to train and manage the problem-prone people. A solid security product alone cannot protect the organization without the implementation of a good management policy. Initiatives in adopting new technologies run into trouble because people may not want change. Since new policies interfere with the employees' way of life, implementing policy based security plan can be very challenging [14].

3.2 Availability of resources

Unlike other investments, information security investments are not intended to earn a profit but to reduce the risk. The investment only succeeds if nothing happens to the information resources and therefore, the benefits are intangible. Growth of spending occurs in a variety of areas such as virus detection, firewall installation, sophisticated encryption techniques, data backups and purchase of hardware devices. Research on information security have focused primarily on technical, physical and behavioral aspects of preventing information security breaches but neglecting economic aspects of information security. Availability of resources for information security has effect on information security based on the fact, that training, purchase of software and hardware, implementation of policies all depend on economic ability of the organization [9].

4.0 Problem definition

Information security in the healthcare sector is a major concern in most health institutions and the adoption of Electronic Health Records point towards a need for better information security [4]. A study done by [19] on electronic health record and cybersecurity challenges indicate that, although EHR guarantees easy access to patients' information, there is a risk of privacy violation and identity theft which leads to patients bearing huge financial consequences and emotional harm. A study done by Ministry of Health in 2011 within Kenyan health facilities that have implemented EHR reveals that only 29% have implemented a 'little' security on their system due to resource constraints. This implies that information insecurity is rampant. It is argued that the baseline of information security is integrating physical, administrative and technical controls. This study seeks to develop an EHR information security model that comprises the administrative, physical and technical controls that will improve the security of EHRs system in hospitals with financial constraints.

5.0 Methodology

This study adopted a cross-sectional exploratory research design which helped in collecting ideas and responses from health facility employees who use EHR which in turn assisted in coming up with an information security model. The study's population was 385 staff out of which 196 respondents were sampled using purposive sampling by [27] formula. A Likert scale structured questionnaire was used to collect data. The study was based at Jaramogi Oginga Odinga Teaching and Referral Hospital (JOOTRH) in Kisumu County, Kenya. This is the largest hospital in the Western region of Kenya serving an approximate 5 million people from Nyanza, Western and part of Rift Valley provinces. It has been in existence for more than 100 years having been established because of the high Malaria presence in the region. It serves Nyanza which has the highest prevalence of HIV at 13.9%, hence high population of patients. Test-Retest method was used to establish reliability of the data collection instrument. A Cronbach's Alpha value of 0.677 was obtained using SPSS. Content validity of the data collection instrument was determined by the Subject Matter Experts (SME) and a content validity ratio of 1 was obtained. Staff at JOOTRH were sensitized on filling the questionnaires. The pilot questionnaires were administered to selected staff two weeks before the real data collection. Team leaders were chosen to help in distributing the questionnaires to their team members. Collected data was analyzed. Correlation analysis was used to establish the relationship between the dependent and independent variables. A Binary Logistic Regression analysis was carried out to establish the strength of relationship between the predictors and the predicted. The outcome of the analysis was a mathematical function to predict the probability of EHR security.

6.0 Results

6.1 EHR security threats and vulnerabilities

[11] security rule establishes minimum security standards for protecting EHRs. The security rule contains administrative, technical and physical security controls that must be put in place to secure patients' information, failure to enforce this will result in many security threats to the system. Analysis indicates several threats to the EHR systems at the health facility. Respondents cite unauthorized access as a major threat to the EHR system with 93.5% of the respondents being positive. Other threats include social engineering (87.2%), theft of records (80.8%), lack of file encryption (79.7%), use of counterfeit software (65.8%), lack of backups (64.2%), lack of input validation (61.5%), blackouts (58.8%), lack of antivirus (54%), access permissions not allocated (52.9%), system breakdowns (52.4%), lack of multi-factor authentication (50.8%), errors due to lack of technical support (49.2%) and lack of staff training at 40%.

6.2 Security controls implemented

The confidentiality, integrity and availability of EHR information depends on the physical, administrative and logical security implemented to secure the EHR system. The health facility implemented minimal safeguards such as multifactor authentication (54.5%), password changed often (78.1%), automatic logoff (63.1%), physical security (94%) and computer sharing (59.4%). Basic safeguards such as having a security professional, allocation of access rights, non-users of the system deleted from the system, power backup and measures to guard unauthorized access had not been implemented.

6.3 Effectiveness of security measures implemented

To establish the effectiveness of security controls implemented at JOOTRH to protect EHR system, questions were developed based on the ISO 27004 standard and the Standards and Guidelines for Electronic Medical Records in Kenya. These questions were directed at finding out whether any implemented security is effective. Respondents were asked whether the implemented security were adequate and were working as expected. They were also asked to specify if the implemented security had protected the EHR system. 97% of the respondents felt physical security implemented

has been effective. Automatic logoff had (46%), password implementation got 36.9%,while multifactor authentication got 29.4%.

6.4 Proposed additional security controls

In regard to which best components could be integrated to the existing security factors, all the respondents (100%) agreed on proper media disposal, privileged account ownership, frequent system audits and identification and authentication techniques as major factors to be implemented to secure the EHR system. 99% of the respondents supported proper system configuration and automated offsite backup followed by enhancement of physical security which had 95.2%. Environmental security which included humidity, leaks and temperature regulation had 94.7% of respondents supporting it, 94.2% supported having enough power backups such as generators and uninterruptible power supply (UPS). System maintenance and personnel security were supported by 92.5% and 92% respectively.

7.0 Determination of effectiveness of Security safeguards

To establish the relationship between EHR system security and the security safeguards, a Spearman's correlation rho (ρ) between the variables was done. A 2-tailed test significance value was used. A correlation coefficient for EHR system security and technical controls was 0.841. It is also indicated that the correlation coefficient for EHR system security and administrative controls is 0.814 while the correlation coefficient between physical controls and EHR security is 0.689. Correlations between predictor variables was weak. Binary logistic regression was used to establish the effect of the safeguards (predictors) on EHR security. Binary logistic regression provides a coefficient "expB" which measures each independent variable's partial contribution to variations in the dependent variable. The EHR system security was the dependent variable with dichotomous responses (i.e secure or insecure). The independent variables were physical, technical and administrative information security controls. The assumptions of this analysis are that data is categorical, no extreme points or outliers exist, the dependent variable is dichotomous and there is a low correlation between the predictor variables. The responses for the variables were transformed into Z-scores for proper interpretation and comparison. Z-scores are standardized deviations from the mean. This study, got responses from staff regarding administrative, physical and technical information security controls which needed interpretation and comparison. The purpose of Z-scores was to identify and describe the exact location of every score in a distribution [20]. To predict the probability outcome of security of EHR, a logit function was developed from predictor variables and the independent variable. Binary logistic regression was done in two steps in SPSS. Block 0 and Block 1. Block 0 helps us understand how good the model is, while Block 1 tables helps in forming the model/function.

		B	S.E.	Wald	df	Sig.	exp(*β*)
Step 1[a]	Zphy_controls	71.808	2589.393	.001	1	.978	1.533
	Ztech_controls	49.486	1847.229	.001	1	.979	3.102
	Zadm_controls	66.958	2406.696	.001	1	.978	1.201
	Constant	-54.006	1896.351	.001	1	.977	.000

Table 1 *Variables in the Equation*

Table 1 gives several variables. The Wald test is used to test the hypothesis that $\beta = 0$. The Wald test is used to eliminate predictor variables that are not significant to the dependent variable. In the Sig column, the *p*-values are all above 0.05 (alpha). The sig. values for physical controls is 0.978, technical=0.9979 and administrative is 0.978. This means that although the correlation test for EHR security and physical, technical and administrative controls was significant, once the other variables are controlled for, one predictor variable will not be significant to secure the EHR system. To interpret the differences between effects of respective EHR security controls to the predicted variable, the exp(β) column which represents the odd ratios for the individual variables is used. It should be noted that:

Probability *(p)* = odd ratio/(1+odd ratio)……eqn (1)

For example, if physical controls are increased by one unit, then they improve the EHR security by 1.533 times. Technical controls improve 3.102 times with an increase of one unit while administrative controls improve EHR security by 1.201 times with a unit increase. Table1 generally gives the magnitude of the effects of the predictor variables are to have on the outcome of the dependent variable. In the model, the β values for each variable are also considered. The co-efficients for the model are contained in the column headed β and are determined using Maximum Likelihood Estimation (MLE). The larger the β value, the greater the effect the predictor variable has on EHR security.

The full model (logit function) being tested is as follows; Logit (p) =

$$logit\ p = \left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \text{eqn (2)}$$

Using algebraic and logarithmic rules, the estimated probability

$$(\hat{p}) = \frac{e^{\beta_0+\beta_1x_1+\beta_2x_2+\beta_3x_3}}{1+e^{\beta_0+\beta_1x_1+\beta_2x_2+\beta_3x_3}} \text{ ..... eqn (3)}$$

Substituting the constant and *B* values:

$$\hat{\mathbf{p}} = \frac{e^{-54.006+71.808x_1+49.486x_2+66.958x_3}}{1+e^{-54.006+71.808x_1+49.486x_2+66.958x_3}} \quad \text{eqn (4)}$$

Where;
$\hat{p}$ is the estimated probability of EHR security.
x_1= Zphy is the physical controls
x_2=Ztech are technical controls
x_3=Zadm are administrative controls

Given the values of x_1, x_2 and x_3 one can predict the probability of the EHR system being secure or insecure. The goal of the logistic regression is to estimate p̂ for a linear combination of the independent variables (x_1, x_2 and x_3). Equation (4) is also called a linear probability model. The estimated probability on the left side has to be a value between zero and one. If the probability is above 0.5 after substituting the values of x_1, x_2 and x_3 then EHR system is secure. The implementation of the security controls can be varied according to the budget of the health facility. This adjustment is done while observing the probability values so that it does not fall below 0.5 or as the organization culture dictates. With the limited resources and funding of government referral hospitals, this model will be of help to achieve EHR security by implementing balanced security safeguards

8.0 Discussions

Personnel training, file access permissions, input validation, user support, social engineering, up-to-date antivirus, multi-factor authentication, system breakdowns, blackouts, backups and genuine software installation were some of the threats and vulnerabilities established. Responses from the respondents ranked file access permission as the biggest threat of information security at the facility. With the use of passwords only, social engineering (87%) which was also listed as a major threat becomes easy for unauthorized users to exploit the system. Health facilities need to ensure authentication is well implemented by using multifactor authentication which utilizes passwords, biometrics, smartcards and usernames. It was also realized that a significant percentage of users have fear over viruses because there was no active antivirus installed on their systems. Antivirus software installations and updates should be outlined in the information security policy for proper security. Backups ensure continuity in cases of disasters, but, 70% of the respondents do not backup their information. Lack of genuine software, blackouts, lack of frequent training and lack of user support were also mentioned as major threats to patient information security with 97% of respondents yearning for change in each case. It was established that physical security, helpdesk, deletion of users from the system have not been well supported. Physical security helps in barring unauthorized users from accessing patients' information while helpdesk helps alleviate errors made by users. If non-users still exist on the system, they create vulnerability for remote access. Respondents confirmed that users who leave the organization, sacked or transferred to other areas are not immediately deleted and their user rights revoked from the system. Majority of users feel the system does not automatically log off users and passwords do not expire. It can be noted that, although a "little" security exists, there is still much that is supposed to be done to protect patients' information. Adequate system documentation helps users sort little problems that pop up during their working. Users feel the password policy has not been strengthened, this is because more than 63% of the users say the still share the passwords. Multi-factor authentication is very important for the EHR system but only 70.6% of the users feel it has been implemented well. Although access rights help in limiting unauthorized users from accessing information that is not relevant to their work, 97% of the users feel it has not been implemented well in the organization. Physical controls have been implemented well (82%) just as indicated in the literature. Power backup does not exist and therefore the system cannot be available all the time. Lastly, 70% of respondents feel the system is not adequately maintained. It can be established that although there are some security controls that were implemented in the hospital, the EHR system is still under threat because most of the controls are not effective. Personnel are responsible for the hardware and software and at the same time, they are the same people working with the EHR system to fulfill the organizational objectives. Personnel therefore are the backbone of the system and need to be protected from system hazards. Ergonomics ensures system optimum performance. Training makes users confident while doing their work and helps in controlling errors. Proper hiring and termination procedures ensure that people of high integrity are hired and that employees are fairly dismissed. People should be protected and cared for so that they do not sabotage the organization. Respondents (86%) agreed that, if proper personnel security is implemented, there would be optimum performance and users will also be sincere in their work. Frequent security assessments help in sealing the loopholes that could create vulnerability in the system.

9.0 Conclusions

This research was conducted at JOOTRH which is one of the government referral hospitals in Kenya serving more than 5 million people in the western, rift valley and Nyanza region. The study established the effect of availability of resources and organizational culture on EHR information security, though most of the characteristics or factors of the two moderating variables were already covered in the predictor variables and therefore were not analyzed separately. This research has demonstrated that no single control is adequate for the security of EHR system. From the model, it can be deduced that physical controls, administrative controls and technical controls when integrated improve security of the EHR system greatly but cannot work independently. It has been established that physical security contributes more to the security of an information system followed by administrative controls then technical controls.

10.0 Recommendations

Training of users both on EHR system use and security helps them to have confidence in the system and also helps alleviate minor mistakes during work. Automated backups help in BCP, while frequent risk analysis establishes weaknesses in the system. Regular system audits ensure that loopholes in the system are detected and any fraud can

also be stopped early enough. Proper hiring and termination procedures involve finding out from the referees what kind of person you are hiring, his past working experiences and behavior. This gives the employer enough information about the candidate before hiring. Proper termination procedures eliminate discontent in employees and help in ensuring security of the system when they leave. Proper system configuration ensures correct assignment of access rights, declaration of who to access, when and how the system should be accessed. These activities should be done keenly to ensure users are not elevated to access rights beyond their work. This should be done using a certain policy established within the organization such as “Deny All or Allow All”. Proper disposal of information resources should be followed to stop dumpster diving attacks. In the scenario of EHR, proper disposal of hardware such as computers, external hard disks and flash disks will control this attack. As a measure of unexpected breakdown of the system, frequent maintenance is required in the organization. Frequent maintenance can help alleviate threats such as war driving and zero day attacks. Personnel are responsible for the hardware and software and at the same time, they are the same people working with the EHR system to fulfill the organizational objectives. Personnel therefore are the backbone of the system and need to be protected from system hazards. Ergonomics ensures system optimum performance. People should be protected and cared for so that they do not sabotage the organization. Blackouts, leaking roofs and other environmental factors such as humidity and extreme temperatures should be avoided in all the circumstances in the computer rooms.

REFERENCES

[1] Adesina, A. O., Agbele, K. K., Februarie, R., Abidoye, A. P., & Nyongesa, H. O. (2011). Ensuring the security and privacy of information in mobile health-care communication systems. South African Journal of Science, 107(9-10), 27-33.

[2] Åhlfeldt, R. M., & Söderström, E. (2010). Patient Safety and Patient Privacy in Information Security from the patient’s view: A Case Study19. Information Security in Distributed Healthcare, 203.

[3] Akanbi, M. and Agaba, E. (2011). Use of Electronic Health Record in Sub-saharan Africa:Progress and challenges. Journal of Medicine in the Tropics, 14(1), p.5.

[4] Appari, A. and Johnson, M. (2010). Information security and privacy in healthcare: current state of research. International Journal of Internet and Enterprise Management. 6(4), p.279.

[5] Bidgoli, H. (2006). Handbook of information security. Hoboken, N.J.: John Wiley.

[6] Business Daily (2017) http://www.businessdailyafrica.com/Insurance-fraud-more-than-triples-to-Sh324-million/-/539552/2978878/-/wcsno2/-/index.html

[7] Fibikova, L. and Mueller, R. (2012). Threats, Risks and the Derived information security strategy. Securing Electronic Business Processes, pp.11-20.

[8] Gao, Xiangzhu et al. "Implementation Of E-Health Record Systems And E-Medical Record Systems In China". The International Technology Management Review 3.2 (2013): 127-139.

[9] Gordon, Lawrence A. and Martin P. Loeb. "The Economics Of Information Security Investment". ACM Transactions on Information and System Security 5.4 (2002): 438-457.

[10] Hartwig, Robert P. "Cyber Risks: The Growing Threat". Global risks 2014 9 (2014): p.5-14.

[11] HIPPA (2008) https://www.nist.gov/healthcare/security/hipaa-security-rule

[12] Juma, K., Matoke, N., Waliaro, A., Wanyembi, G. AND Ogao, P. (2012). Current Status of e-health in Kenya and Emerging Global Trends. International Journal of Information and Communication Technology Research, 2(1).

[13] Kritzinger, E. and Solms, S. (2013). A Framework for Cyber Security in Africa. JIACS, Vol. 3, pp.1-10.

[14] Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009, December). Exploring the relationship between organizational culture and information security culture. In Australian information security management conference (p. 12).

[15] Muga, Richard et al. "Overview Of The Health Systems In Kenya". Kenya Health System Description. 1st ed. Nairobi: Ministry of Health, 2010. 9-15.

[16] Mugo, D. and Nzuki, D. (2014). Determinants of Electronic Health in Developing Countries. International Journal of Arts and Commerce, 3(3), p.3-4.

[17] National Institute of Standards and Technology, (2012). Performance measurement guide for information security. NIST special publication. Gaithersburg: NIST.

[18] Omotosho, A. and Emuoyibofarhe, J. (2014). A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records. IJAIS, 7(8), pp.11-18.

[19] Onuiri, E., Idowu, S. and Oyindolapo, K. (2015). Electronic Health Record Systems and CyberSecurity Challenges. International Conference on African Development Issues. [online] Available at: http://eprints.covenantuniversity.edu.ng/5326/1/Paper%2054.pdf [Accessed 16 Feb. 2016].

[20] Salkind, Neil J and Kristin Rasmussen. Encyclopedia Of Measurement And Statistics. 1st ed. Thousand Oaks, Calif.: SAGE Publications, 2007. p.5.

[21] Sattarova, F. and Kim, T. (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and

Ubiquitous Engineering, 2(2), p.5.

[22] Sellars, C., & Easey, D. A. (2008). Electronic health records: data protection issues in Europe. BNA International, BNA's World Data Protection Report April.

[23] Smith, B., Austin, A., Brown, M., King, J., Lankford, J., Meneely, A. and Williams, L. (2014). Challenges for protecting the privacy of health information: Required certification can leave common vulnerabilities undetected. Management of Computing and Information Systems. Available at: http://www.hhs.gov/healthit/healthnetwork/background/ [Accessed 6 Jun. 2016].

[24] Sood, S., Nwabueze, S., Mbarika, V., Prakash, N., Chatterjee, S., Ray, P. and Mishra, S. (2008). Electronic Medical Records: A Review Comparing the Challenges in Developed and Developing Countries. Hawaii International Conference on System Sciences. [online] Available at: https://www.computer.org/csdl/proceedings/hicss/2008/3075/00/30750248.pdf.

[25] Thompson, L. (2013) Data breach and encryption handbook. Chicago: ABA Publishing.

[26] Yamane, Taro. 1967. Statistics, An Introductory Analysis, 2nd Ed., New York: Harper and Row.

Professor Antony J. Rodrigues
Anthony J. Rodrigues is Professor of Computer Science at the School of Informatics and Innovative Systems and Director ICT, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya. His research interests include Computational Mathematics, Systems Modelling and IT & Society Policies. He has been involved in the design and development of robust integrated management information systems for universities.

Dr. Silvance O. Abeka
Dr. Abeka is a senior lecturer and a Dean- SIIS of JOOUST. He was a Director- Institute of Open and Distance Learning at Africa Nazarene University and a Dean- Faculty of Applied Science and Technology of Kampala International University- Dar-es Salaam College. His research interests include IT innovation adoption, open source software study, IT offshoring, Management Information Systems, Network and System Security, Digital Technologies impact on Society, Networking Protocols and Topologies, Web- Design and E- Learning Technologies.

Dr. Solomon Ogara
Dr. Ogara is currently a senior lecturer and Chair of the Department of Computer Science and Software Engineering in the School of Informatics and Innovative Systems at Jaramogi Oginga Odinga University of Science and Technology, Bondo –Kenya. He has also served as the a post-graduate representative for the school. Previously, Dr. Ogara served as a visiting professor at DeVry University (USA) and assistant professor at Livingstone College (USA). Dr. Ogara has more than 15 years experience in the Information Technology field with specific interest in IT security, IT Forensics and Cyber-Security.

Everleen Nekesa Wanyonyi
Nekesa is an MSc student at JOUST Bondo, Kenya majoring in Information Technology security and forensics audit. She has a BSc in Information Technology from KCA university, Kenya and a Kenya National Examination Council (K.N.E.C) diploma in Computer Studies from Kisumu National Polytechnic. She has a major interest in Electronic Health Records security. Nekesa is a senior computer technologist at Maseno university, Kisumu, Kenya.