SECURITY CONTROL MODEL FOR ELECTRONIC HEALTH RECORDS:

A STUDY OF MOI TEACHING AND REFERRAL HOSPITAL-KENYA

KEMBOI LUCY

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN HEALTH SYSTEMS AND INFORMATICS, DEPARTMENT OF INFORMATICS AND INFORMATION SCIENCE, RONGO UNIVERSITY

2020

DECLARATION AND APPROVAL

DECLARATION BY THE STUDENT

This thesis is my original work and has not been presented in any other university or any other institution of higher learning.

Sign: ………………………………………. Date: ……………………………………….

Lucy Kemboi

MHI/6404/2015

DECLARATION BY THE SUPERVISORS

This thesis has been submitted for examination with our approval as the university supervisors;

1. Sign ……………………………………… Date: ………………………………………...

Dr. James Abila

Senior Lecturer Department of Informatics and Information Science

Rongo University

2. Sign….………………………………Date: ……………………………………...........

Dr. Lamek Ronoh

Senior Lecturer Department of Informatics and Information Science

Rongo University

DEDICATION

I dedicate this work to my late Dad Thomas Kemboi for encouraging me to scale the heights of education, husband Peter and my children Megan and Keegan for their, prayers, understanding and encouragement throughout my study.

ACKNOWLEDGEMENT

First and foremost, I would like to thank the almighty God, for his favors and blessings throughout my study. I recognize the immense contribution of my supervisors Dr. James Abila and Dr. Lamek Ronoh for their commitment, dedication, support and guidance they accorded me throughout my study. I acknowledge my colleagues and fellow students Kelvin, Silas, Rinnie, Kate and Rose who in one way or another contributed immensely to my studies by updating me through phone calls and encouragement throughout my study.

My sincere thanks and acknowledgement to the respondents who took their time and effort to answer the questionnaires and provided me with the information that made this thesis a success.

ABSTRACT

Secure Electronic Health Records (EHR) is essential in provision of reliable information to support delivery of healthcare services. The adoption of (EHR) provides improved patient care that is more efficient. The use of EHR raises concerns over protection of patient's information. Therefore, there is need of a security control model of Electronic health records in the expanded environment. This study developed a model that ensures that 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 study was guided by three research objectives: To examine security controls of the current EHR system, establish the security controls requirements and to model a security control model for EHR for MTRH. This study was also guided by Systems Theory formulated on the relationship between independent variables and dependent variables on enforcing information security on Technical, Administrative and physical security controls in managing risks, internal process controls and information auditing. The study adopted a cross sectional survey study design on security of patient's health records with a target population of 200 health records MTRH members of staff working in 8 departments and handling patient's health information, with a sample size of 133. A three-level questionnaire with both structured and unstructured questions with five-point scale chart was used. The data collected was coded, entered and analyzed using the statistical package for social sciences (SPSS). The summarized data was presented in percentages and frequency distribution tables, charts and graphs. The study findings showed that the administrative Security controls were well articulated in MTRH (60%) compared to Technical (36%) and Physical security controls (32%). Therefore, the study recommended a security control model that secures EHR for MTRH. This is represented by the three-security control in equal measure. 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.

TABLE OF CONTENT

LIST OF TABLES

LIST FIGURES

ACRONYMS AND ABBREVIATIONS

AMRS	Automated Medical Research System
CDI	Constrained Data Item
CIOs	Chief information officers
CSP	Cloud Service Providers
DHMIS	District Health Management Information System
EHR	Electronic Healthcare Records
EMR	Electronic Medical Records
EPR	Electronic Patient Records
e-PHI	Electronic Protected Health Information
HIT	Hospital Information Technology
HMIS	Health Management information System
I-HMIS	Integrated Hospital Management Information System
INFOSEC	Information Security
IQ CARE	International Quality Care
IREC	Institutional Research Ethics Committee
ISO	International Organizational for standardization
MOH	Ministry of Health

MTRH	Moi Teaching and Referral Hospital
NIST	National Institute of Standards and Technology
PR	Patient Record
PHI	Protected Health Information
SOA	Service-Oriented Architecture
SPSS	Statistical Package for Social Science
RHIO	Regional Health information Organization
VPN	Virtual Private Network
SIEM	Security Information and event Management
UDI	Unconstrained Data item
WHO	World Health Organization

DEFINITION OF TERMS

TERMS	DEFINITION
Availability	Authorized users that have access to the system.
Confidentiality	EHR Data is protected from unauthorized view.
Electronic Health Records	The Patient information stored away digitally.
Integrity	Is maintaining consistency, accuracy and trustworthiness od data over its entire life cycle.
Security Control	Security measures that detect, counteract, or minimize security risks to information and computer systems.
Security Control Model	A framework in which a security policy is developed is developed and built within the confines of information Security in terms of Technical, physical and Administrative security controls.

CHAPTER ONE: INTRODUCTION

1.1 Background to the Study

Health system is the sum total of all associations, organizations, and assets whose main role is to improve health. A good health system requires a robust financing component, a well-prepared and sufficiently paid workforce, dependable information system, good leadership and governance, good service delivery and access to essential medicine. Health Management Information System is an information system specially designed to assist in the management and planning of health programmes, as opposed to delivery of care (WHO, 2010).

Moi teaching and referral hospital has always used manual medical records from way back in 1917 when it was a cottage hospital. Records were manually created, and have been shifting from one system to another. In October 2009, the hospital adopted the Automated Medical Records System (AMRS) registration module in all OPDs registration units.

Funsoft software was adopted by MTRH, in 2010 for management of health records. However, over the years, MTRH has faced greatest challenges in information Security breaches that are prevalent while dealing with IT service providers as third parties as a result of inadequate security measures in the associated third-party agreements. This system was originally started by Indiana University in collaboration with Moi University in 2002 in AMPATH Centre. The system did not replace the manual registration system but instead worked hand in hand as a backup in times of electronic system failure

(MTRH Strategic Plan 2005-2010). The hospital has introduced a more integrated electronic health records system commonly known as HMIS capable of electronically managing health information system (fun-soft) with the aim of automating the outpatient services to improve the management of patient’s medical records (MTRH Strategic Plan 2008-2012).

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. However, the hospital faces challenges in information security of the Electronic Health records by virtual attacks as well as potential threats. MTRH also faces information security challenges on, physical, technical and administrative security controls. This is because of the physical failure of infrastructure, damaged from “natural or environmental hazards, and unauthorized access by personnel or external parties.

These systems have encountered challenges of laptops being stolen, leading to delay in safety of patient’s information. The infrastructure has been inadequate because of frail or missing Wi-Fi signals and poor network signal, making it difficult for network connectivity. There has been lack of electric power in some areas making it impossible to access the systems (Muinga *et, al.,* 2018).

1.2 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 (MOH, 2014). The Kenya Health sector referral implementation guidelines encourages Promotion of linkages across the different levels of care between public and private hospitals to improve the health system's ability to transfer clients, client parameters, specimens and expertise between the different levels of the health care system from the national health referral Services (level 6) to county referral hospital (level 4 and 5). Therefore, all facilities are required to invest in basic information and communication technology to support consultations and ensure proper back-up and e-referrals.

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, leading to leak in patient information, medical fraud, serious legal implication and financial constrain. Majority of the information security breaches 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 (Fernandes *et, al.,* 2013).

Local hospitals in Kenya lack 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 referred to as INFOSEC (Information security), they are the processes and methodologies involved with keeping information confidential, available, and assuring its integrity. It also refers to: Access controls, which prevent unauthorized personnel from entering or accessing a system. Security control model that ensures that the security of the electronic health records is well managed and can be adequately assured if the emphasis goes beyond administrative controls and incorporates technical security controls and physical controls.

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). Security control model is the required to ensure to that 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 conforms 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 (Chukkapalli *et, al*., 2020).

1.3 Purpose of the study

The purpose of the study was to model security control system for EHR in MTRH.

1.4 Study Objectives

I. To assess security controls of the current Electronic health records system.

II. To establish security control requirements for MTRH.

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

1.5 Research Questions

I. What security controls do the current Electronic health records have?

II. What are the EHR security requirements for MTRH?

III. Which model can secure EHR system for MTRH?

1.6 Justification of the study

The Kenya national eHealth policy 2016-2030 on approach and policy orientation on assets and resources shows that there is absence of adequate infrastructure to support quality, a rapid Internet connection which is one of the reasons for poor take up of eHealth applications in the country and in remote regions. This arrangement requires policymakers in the ministries of health, and information technology to collaborate in identifying effective ways of improving infrastructure (MOH, 2012). The study is beneficial to MTRH and other hospitals that have adopted the Electronic Health Records by providing them with perspectives of looking at security concerns within the EHR system. This way the management of MTRH and its clients who are the patients are able to make better decisions based on the findings of this study. Hence providing all the stake holders with the understandings of security concerns of the security control model. The study would benefit MTRH among other hospitals that and cost of network access to ensure easier transfer of health information, by developing Electronic Health Records (EHR) measures and rules that controls how data is captured from patients.

1.7 Significance of this study

This study is beneficial to the ministry of health and enable them achieve the goals on information generation, validation, analysis, dissemination and utilization of the health information (KHSSP 2013-2017).

It is beneficial to the Ministerial Strategic and investment plan (2012-2017) guided by the Kenya Health Policy (2014-2030) and the vision 2030 under the health information pillar with the aim of accomplishing the highest possible standard of health in a responsive way.

This study adds more knowledge to the devolution of health in Kenya through the information pillar will bring services closer to the people and improve efficiency and promote accountability. It enables a good referral system with a comprehensive management of patients' records and ensure proper recording of all referrals and create referral links in different levels of care from the national teaching referral hospitals cascaded and networked through to the community health services as indicated by the Kenya Health Sector Referral Guidelines (2012).

This security model ensures that there is growth of health data sharing and enhance patient care, reduce readmission, avoid medication errors and decrease duplicate testing. The health information principle there will be a reduction of burden of violence and injustice, strengthened collaboration with other health related sectors leading to improved health.

It leads to a good organization structure for authorizing great data security good information security, full user awareness and responsibility towards information security and the important approaches, policies, procedures, processes, technologies and compliance enforcement mechanisms to ensure that confidentiality, integrity, availability of the hospital electronic assets or information are maintained at all times.

1.8 Scope of the study

The study focused on designing a security model for EHR at MTRH by Examining the current security controls for MTRH and establishing the security controls for EHR at MTRH.

1.9 Limitation

It took longer to meet the sample size of 133, since the 200 health records staffs are usually in shifts, off or on leave. There were members of staff holding vital information from the researcher for fear of being exposed or maybe some might think that the researcher was intruding on their privacy. This limitation was managed making a clarification that the research was confidential.

1.9.1 Delimitation

This study was delimited to the department's handling patient's health records with a population of 200 members of staff. The departments that were not investigated were those that do not handle patient's health records like finance and procurement department. The tool used were the questionnaires to gather information within the shortest time possible.

1.9.2 Assumption of the study

The study assumed that a security control model would ensure a secure EHR by making the system available to authorized people, would be confidential. It was also assumed that information given by the respondents in the questionnaire was a true reflection of the reality at the hospital.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The objective of mHealth in Kenya is to guarantee that the design, development and execution of interoperable, scalable, sustainable mHealth solutions benefits clients and healthcare service specialists in a cohesive and holistic way. The mHealth should provide a regulatory structure that will empower coordination and implementation of vigorous mhealth solutions (MOH 2017).

The standardization will develop communication protocol, gadget interfaces, applications and working systems that will 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, also serves as an alert and early warning capability, 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 (WHO, 2010).

Health Management Information System (HMIS) incorporates and reports the exercises of the network of health care professionals, facilities and the administrative and logistic information needed to sustain them. The adoption of electronic health records (EHR) and other developments offer opportunities for improved patient care and increasingly efficient practice management. In any case, as growing amounts of individual medical information are stored in electronic format, ensuring the protection the privacy and security of this information and guaranteeing the integrity of EHRs is very critical. The web based EHR systems enables patient to remote access to their whole medical history whenever. Hence security and protection of delicate information will be critical to the successful administration. For adaptation of EHR, the key factors are improvement of quality care, efficiency, patient's safety, the state of technology, and organizational influences (Zhang, 2010).

Globally, Denmark is viewed as a leading nation as far as eHealth integration and healthcare services delivery (Kierkegaard, 2013). Denmark has secure intranets that have been setup to link areas with local health authorities and other associations through secure intranets. This has been cultivated through virtual private network (VPN) connections to create an Internet based healthcare data network. The national association known as MedCom was developed in Denmark in 1994 with the role of certifying systems (from various computer organizations and sellers) that are able to interconnect on the national network which Medcom oversees. Electronic health records are currently utilized by practically all broad practitioners in Denmark at 100% penetration, roughly, 74% by full time experts and all drug store. Every single General Practitioners and healthcare institutions have access to the Danish Health Data Network. 80% of all healthcare correspondences in the essential healthcare sector are being exchanged through electronic data interchange (EDI), with millions of standardized medical documents being exchanged every month (Kushniruk, *et al*., 2010).

The push for eHealth adoption over the previous 20 years in the Danish health sector has prompted the organizations to use several eHealth technologies. However, the Danish healthcare experiences eHealth system fragmentation which has prompted to eHealth's inability to achieve maximum capacity in delivering quality healthcare service. In a situation a cancer patient whose information got lost three times between hospital departments. His treatment was postponed and when the patient was offered chemotherapy, he was already too frail to receive the treatment and died shortly a while later. The Danish Health and Medicines Authority reported that there had been 26 cases amid that quartile due to failure of transferring the appropriate clinical information. The Danish Medical Association and Danish Nurses' Organization accused the healthcare services failure of transferring patient records to the numerous EMR systems into a functional national system (Kierkegard, 2013).

Denmark's forceful push for eHealth systems has prompted to disruptions in practitioners' work process. The portable nature of healthcare work requires practitioners to continuously access several workstations within the same care organization which expects them to over and over again sign-in several times during the day and often update their passwords (Christiansen and Nøhr 2011). To spare time, healthcare practitioners share passwords and do not sign out of a workstation with the end goal of others to utilize it. Clinicians may have utilized this way to deal with counter impacts of frequent change of passwords which expands the burden on human memory and decrease the probability of reviewing a specific password when the number of passwords they have to memorize increases and they have to recollect up to five random passwords (Brumen, 2017). Despite the fact that there is a sense of urgency for practitioners to rapidly access the patients' medical records, the present practices of sharing passwords and neglecting to sign out of workstations have traded off the security and protection of a patient's delicate information. At the same time, it makes it hard to perform review trails and decide the identity of the individual accessing and altering the restored medical records. This means "that the way in which information rupture happens becomes progressively hard to avoid and follow. Denmark has so far been blessed in this issue as the 2010 Annual Report by the Data Surveillance Board demonstrated that only 4 % of revealed breach cases were related to the health sector (medical companies, clinics and physicians (Kierkegaard, 2013). Therefore, the system guarantees that client's information is handled in a safe way by setting up mechanisms that ensures privacy, confidentiality, integrity, availability and non-repudiation at all times. The data should be secure in transit and when archived.

Regionally, in Zambia Smart-care was created to address the issues of the Ministry of Health in the care of HIV patients, thinking of the dimension of the foundation advancement in the health sector in Zambia (CDC, 2010). In 2006, after two years of effective pilot tests, Mweebo (2014) endorsed smart-care as the sole electronic medical record to be utilized for public and private health care in Zambia. The primary point of the smart-care program was to connect up services for HIV clients and improve access to health information regardless of area, thereby, diminishing delays in commencements of treatment, duplication of examinations, dangers and mistakes, costs and improving HIV data standards, security and confidentiality in the nation (Neame ,2013).

The smart-care program contains electronic forms that clinicians use to record patient information that incorporates counseling, testing, staring history and physical examination, investigations, medicines and long-term development (WHO, 2016). The way of protecting the confidentiality and integrity of patient information is presently a lawful necessity that healthcare establishments should fulfill (Neame, 2013). Be as it may, still remains as one of the primary difficulties associated with EMR. Patient privacy is important because exposure of personal health information such as HIV status in the case of smart-care could result in social stigma, loss of work and refusal of health benefits (Tian-Fu *et al*., 2013). Likewise, unapproved access may result in patients experiencing monetary misfortunes unlawfully billing information may result in patients suffering financial losses from illegal transfer of funds. EMR such as smart-care should consolidate security features that ensure against misuse by approved users, hackers and those who steal the personality of patients (Tian-Fu *et al.*, 2013). The smart-care EMR met the physical safeguards because all the equipment's were put away in lockable offices and screening rooms (Mweebo, 2014). However, the program still had difficulties to address technical safeguards. In perspective of the numerous 36 diverse staff categories who work in the program, there were concerns about abuse of patient information by authorized health staff who work on the program.

To address this need, Neame (2013) supported for the role-based access control (RBAC) to limit access to information that is only relevant to each cadre, for example, only demographic data for a registry clerk. Smart-care has no security highlight to address data transmission such as secure socket layer or encryption. The utilization of ordinary antivirus instead of specialized software based on security information and event management (SIEM) that can ensure that the network and the system infrastructure against cyber hackers remains a major security concern for smart-care.

Locally, the Kenyan government, working with universal partners and local organizations, built up an eHealth strategy, with specified standards, and rules for electronic health record adoption 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 Kenya EMR and International Quality Care Health Management Information Systems, for foreseeing 600 HIV clinics across the country.

The DHIS2 system was actualized as a reaction to the difficulties to the with the past Microsoft Excel file-based system. These incorporated a failure to completely analyze the data collected because of the manner in which the data were aggregated, an absence of error-checking abilities, incomplete data, and in adequate of information and restricted limitation of data for decision making (Muinga *et al*., 2018).

Kenya EMR (OpenMRS 2016) is an Open Medical Record System (OpenMRS) that is broadly used in few African nations to help the administration of HIV/AIDS patients and different ailments such as tuberculosis and other non-communicable diseases. OpenMRS was created to allow flexibility to incorporate contingent upon the requirements, depending on the needs of the health care facilities where the software was to be introduced (Muinga *et. al*., 2018).

International Quality Care (IQ) Care is a Windows-based EHR application system that offers assortment of highlights for overseeing clinical care for essentially HIV or AIDS patients and has been deployed in over 300 facilities in Kenya. The system likewise has a production chain management feature for management of drugs. IQ Care was implemented in Kenya through the support of the Palladium Group (formerly Futures Group) and is donor-funded system through AIDS Relief. Palladium is an international consulting firm that works in various industries to provide customized solutions. In Kenya, they work intimately with the MOH in a scope of health areas including HIV and AIDS and more generally providing strategic information capacity building.

Referral hospitals with m-Health systems ensures that the Health Information Exchange allows patients and professional to safely share indispensable data electronically, the demand for electronic health information exchange between one health care to another is growing along with efforts to improve quality, security and efficiency of healthcare conveyance (MOH,2017).

The benefits of health information exchange is to improve the of quality and safety of patients care and reduction of medical errors, consumer and patient’s education and involvement of their own care , leading to increase in efficiency and elimination of unnecessary paperwork, providing interoperability among electronic health records maintained by individuals, ensuring healthcare personnel have clinical decisions support tools for more effective care and treatment and reducing health related expenses.

MTRH is yet to document and administer the logon ID in a secure manner in terms of user access. There is Lack of offshore backup for disaster recovery, Misuse of access rights and privileges, external and internal hacking of systems, expensive licensing demands, erratic power supply. The network equipment's and servers are yet to be protected against damage, unauthorized access and theft, secure wiring closets and protection of cabling conduits and network switches, portable devices. Terminations or change of responsibilities of employees or third-party providers could result in a security violation due to lack of a predefined management procedure for terminations or changes in responsibilities, leading to an unauthorized access to information systems.

Users whose responsibilities have change or no longer use the system still retain access to the information system. Lack of consistent logging and monitoring mechanisms enables the continued unauthorized information processing activities to occur undetected. Absence of clear segregation of duties compromises the integrity of the processes. The Fun soft system prone to

insecurity for lack of proper controls thus enabling access to information by unauthorized persons. Viruses and Malware have not been adequately taken into consideration. (MTRH guideline for ICT 2016).

This chapter reviews the literature on theoretical foundation of this study, concept of information security and security control models of Electronic Health Records. The chapter also shows the conceptual framework that shows the relationship of the variables to achieve the outcome.

2.2. Secure Electronic Health Record

The Electronic Health Record (EHR) is characterized as digitally stored health care information about an individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times and the IT infrastructure that allows sharing of medical information. Electronic health system describes the software of facts and communication technologies throughout the complete range of function that impact of the Personal Health Information (PHI). Patient Records (PRs) are any information related to patients that are accumulated at some point of the care. Electronic Patient Record (EPR) approaches any patient record that can be accessible electronically. Technology has the potential to move healthcare services to an additional proactive and consumer-oriented model of care and improve the cost, quality, and availability of healthcare services. Electronic patient records decrease the errors of treatment by method of empowering patients to consent with their course of treatment and providing communication channels between patients and healthcare professionals.

The EPR will strength the position of the patient because they will have more and easier control over their health information and can follow the development of their very own illnesses. The EHR serves as the central database where physicians orders for lab x-rays and other lab tests, the EHR enables the hospital and the physicians the ability to track the information they need to follow the insurance companies and federal regulation (Seymour *et.*, *al* 2014).

Health Management Systems is a coordination of healthcare, business management, and information systems. As the healthcare delivery system is held to accountability, healthcare providers and entities must exhibit quality results, financial obligation, and efficient and productive and compelling practices. To do this, health management systems experts gather and investigate data, incorporate innovative management strategies, and utilize new advancements to reengineer healthcare. Health management systems experts are the creators and trend-setters, innovators, and entrepreneurs for the continually advancing healthcare delivery system.

Generally, the use of hospital information systems has many numerous focal points for healthcare providers and patients. 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, (Robert & Wilkinson 2013).

The NIST SP 800-30 is another technique, in which the proposals of the National Institute of Standards and Technology have been considered as a rule for a comprehensive risk assessment program. In this technique, the procedure of risk evaluation is the first phase of the process of security risk administration and incorporates nine stages: system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, and results documentation. Cyber security dangers present serious financial and national security challenges in the 21st century. This has shown that there is a mass of destruction since its damages are real with individuals stealing, changing or destroying information. Modern criminals are focusing on most valuable corporate and governmental information resources by exploiting vulnerabilities in the systems and exploiting absence of security and laxity in security issues inside the organization. Hartwig and Wilkinson (2015) found that larger part of data breaches in the year 2013 affected 43.8% of medical/healthcare organizations compared to 34% of the business segment organizations.

Security and protection executions are specific, Privacy is handling policy, but security is managing the tools to implement the policy. Tian-Fu *et al*., (2013) 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. Wang *et al*., (2014) portrayed 'those allowing cloud service that are not in indistinguishable confined areas from big enterprise users, to take care of confidential personal data of users, which can make potential security and privacy risks. To keep user data confidential against untrusted path by applying cryptographic methods, by sharing decryption keys only with authorized users.

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 (Fernández-Alemán *et al.*, 2013). As a feature of the IT industry Cloud Computing is making quick progress. Alongside advantages of this innovation credit dangers exist (Sotto *et al.,* 2010). 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 (Alotaibi & Federico, 2017). New techniques, for example methods dependent on quantitative research, financial analysis, and statistical models of patient protection, public policy, risk management and the effect of Health Information Technology on medical errors were considered and to check the quality of healthcare provided with the guide of two AHP and TOPSIS approaches, two investigations were done entitled Quality of health care services by using fuzzy AHP approach and approach combining the fuzzy AHP and fuzzy TOPSIS based on strategic review of electronic services quality in the health care industry (Büyüközkan *et al.,* 2011).

Peikari *et., al* (2018) states that the protection of information represents a growing challenge and that poor patient information security represents a major problem that must be addressed with increasingly advanced hospital information technology (HIT). Based on security threats analysis the use of security control module provides security enabled HIS (Health Information System) proxy module, two-way authentication module and one-time password. It is progressively hard to safeguard trustworthiness of digital radiology images and shield them from unauthorized manipulation. Furthermore, the developing integration of complex hospital information systems and the widespread use of mobile devices and the expanding measures correspondence between health care providers require special attention regarding information security (Chen *et al.,* 2019).

Similar to other organizations, healthcare organizations are in danger of information security threats. Meanwhile, they are urged to utilize and share electronic health information. They are especially vulnerable targets for data breaches due to the value of health information. Therefore, securing health information seems to be more challenging than before in the healthcare organizations (Mehraeen *et al.,* 2013). 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 controlled.

In 2014, Insurance Information Institute in the United States of America reported that 783 data breaches hit business at (33.3%) and medical/healthcare organizations (42.5%), (Hartwig and Wilkinson 2015).

Although numerous efforts have been made to arrange information security threats, particularly in the healthcare area, there are still numerous unknown dangers which may undermine the security of health information and their resources, (Bakhtiyarishahri and Zuraini 2012).

Samadbeik, *et al.,* (2015), uncovered that user name and password were the most significant techniques to verify the nurses, with mean percent of 95% and 80%, respectively, 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 studied about the levels of information security protection and security requirements.

Patients private information is needed to provide care, protected information, the basic tools and technique used to maintain medical information security and patient’s privacy, this includes physical safeguards such as computer violations, technical such as firewall and secure transmission mode and administration safeguards including documentation and security policies (Andriole, 2014). In 2014, Insurance Information Institute in the United States of America reported that 783 information breaks hit business (33.3%) and medical/healthcare organizations (42.5%), (Hartwig & Wilkinson (2015). In 2013, Cisco revealed that 99% of Android gadgets were targeted by mobile malware and 71% of Android users experienced all types of web-delivered malware, (Cisco, 2014). In another report about cyber security patterns and difficulties, it was uncovered that in 2014, 64% of organizations showed that their security infrastructure was modern and constantly upgraded. Never the less, in 2015, that number decreased to 59% (Cisco, 2016). This proof demonstrates that organizations are facing a greater attack surface, the developing multiplication and advancement of attack models, and more complexity inside the network.

Like other organizations, healthcare organizations are in danger of information security threats. Meanwhile, they are urged to utilize and share electronic health information. “They are especially helpless targets for data breaches due to the estimation of health information. Therefore, securing health information seems to be more challenging than before in the healthcare (Mehraeen & Ayatollahi 2016).

Donahue & Rahman (2012) 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 (Sharifian & Nematollahi 2013). Improving information security will expand the confidence of patients and clinicians, and may prompt the better utilization of the health data (Datta & Banerjee 2010).

Although numerous efforts have been made to characterize information security threats, particularly in the healthcare area, there are still many unknown dangers which may risk the security of health information and their assets. the most known risks to the information security are unapproved utilization of software and computers for communications and illegal exercises (Bakhtiyarishahri and Zuraini (2012).

Security, privacy, efficiency, and scalability concerns are hindering the wide adoption of the cloud technology, Thus, there is an immediate need for a holistic solution that balances all the contradicting requirements. Therefore, it is essential to recognize the information security risks in hospitals to be able to cope with the potential harms in the future. In fact, to limit losses brought about by a variety of security dangers, information security risk management is vital, and the motivation behind information security risk management is to protect the security in the systems which stores, processes, or transfers organizational information. In order to deal with the risks, there should be an arrangement to assess the severity of threats and to decide the potential risks. Actually, the procedure of risk assessment or risk analysis is the first step in the process of risk management (Al-Issa, Ottom & Tamrawi, 2019).

Information security is about shielding information from mishaps, breaches or other events that could make it harder to comprehend the information. It is practiced in organizations that will in general depend on information and a specific absence of information could harm the organization. This means that information security is important to all organization.

Information security can be characterized as having the correct information, provided to the right person, at the right time and the right place. The patient record Act of Sweden emphasizes the need to ensure the security and protection of patients records (Åhlfeldt & Soderstrom 2010). The United Nations (UN) urges nations to administer for EHR protection and to guarantee that patients are protected after revealing their health information. By authorizing the Data Protection Directive in 1995, the UN was to guarantee that patients' information is utilized within their countries of collection and patient's privacy is ensured (Adesina *et al.*, 2011).

Information security improves the confidentiality and the use of information Security in shaping the biomedical data to achieve these goals, security requirements and information governance in particular and a strong influence on the trajectories and outcomes of data sharing leads to security vulnerabilities in health information systems demonstrated that considering them to be effective in security control of health care centers, there must be contribution of software execution of health information systems（Tempini and Leonelli , 2018).

Hacking a hospital workstation, that is connected to the internet is sufficient enough to gain access to patient information. consequently, information honesty can be undermined by hackers, it is critical to distinguish the information security risks in hospitals to be able to have options to adapt to the potential damages and to limit losses caused by an assortment of security threats, information security risk management is fundamental and hackers have acquired access to servers with medical data previously (Dupler, 2011). They have additionally gotten the access by stealing laptops with patient records of millions of patients Concerning integrity, it is commonly easier to change a digital document, than to change a paper report, as changes on paper are more noticeable and physical access is required to be able to make the change (Burrell, 2011).

Information and communication technology have made excellent development in over the past few years in the field of medicine and healthcare. Healthcare is always undergoing changes, with new technologies, business models and research findings. The necessities for security and privacy are also very critical and very difficult to satisfy in case of Electronic Health Records (EHRs) data particularly when contrasted to any other data. This is because of the clashing needs of clinicians (who request open and simple access to databases) and the patients (who prefer closed and private access to information stored in databases. There are worries on health information security on issues, for example, keeping up classified and maintaining confidential and preventing unapproved access to clinical data on data entry, storage, use, and exchange (Farzandipour, *et al*., 2010).

Therefore, security manages three aspects; to be specific, securing patients' information privacy, guaranteeing data integrity, as well as assuring data availability. Inability to adhere to this may cause various problems, such as legal issues or financial related issues for hospitals and health care providers (Roxana *et al.*, (2013). By improving information security there will be an expansion in the confidence of patients and clinicians, and may prompt to the better utilization of the health data (Donahue & Rahman, 2012). The main reason of information security risk management is to ensure the security in the systems which stores, processes, or transfers organizational information in order to manage the risks, there should be an arrangement to evaluate the severity of threats and to determine the potential risks (Daigrepont and McGrath 2011).

In Hong Kong, Gao, Xiangzhu *et al*. (2013) 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.

In Iran in spite of a number of studies that have been conducted about the information security in hospitals, few studies concentrated on assessing health information security hazards and fundamental factors and underlying causes of them (Zarei and Sadoughi, 2016).

Juma *et al.,* (2012) states the requirement for research and development of an effective information security model to ensure that the patient’s information is protected in Kenyan hospitals which will moderate accountability in handling patient’s information. In this investigation, we built up an EHR system security model that is used to enhance the security of the EHR on an insignificant spending plan in public referral hospitals.

In Africa, Akanbi and Agaba (2011) realized, that the executions of EHR systems frequently depend on international aid, making sustainability, security and improvement very difficult. There is fear that both the physician and patient may be exposed to the world through the use of the web (Mugo & Nzuki, 2014). Juma, *et al.,* (2012), suggested the need for research and development of an effective information security model to ensure the protection of patient’s information in Kenyan hospitals which will mitigate lack of accountability in handling patient’s information. In this investigation, we build up, an EHR system security model that will be utilized to improve the security of the EHR at MTRH. This literature review concentrates on how information security guarantees 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 when staff members are transferred or dismissed.

2.3 Security Control Models.

2.3.1 Bell—LaPadula Confidentiality Model

It was the first mathematical model with a multilevel security policy that is used to define the concept of a secure state machine and models of access and outlined rules of access. 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 Bell-Lapadula model is a security rule (no read up rule): It states that a subject at a given security level cannot read data that resides at a higher security level. Star property rule (no write down rule): It states that a subject in a given security level cannot write information to a lower security level. Strong star property rule: It states a subject that has read and write capabilities can only perform those functions at the same security level, nothing higher and nothing lower.

2.3.2 Clark—Wilson Integrity Model

It was developed after Biba and addresses the integrity of information. This model 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 Clark – Wilson model is to prevent unauthorized users from making modification, separating of duties and preventing unauthorized users from making improper modifications.

2.3.3 Harrison—Ruzzo—Ullman Model

The HRU security model (Harrison, Ruzzo, Ullman model) is an operating system level computer security model which deals with the integrity of access rights in the system. The system is based around the idea of a finite set of procedures being available to edit the access rights of a subject s on an object. The model also deals with the possibilities and limitations of proving safety of a system using.

The three main patient’s information security controls 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 (Kruse et., al 2017)

To investigate information security in hospitals, three main safeguards should be considered (Ray & Newell 2010).

2.4 Technical Security

Technical specialized safeguard deals with “managing access to computer system information and ensure interchanges when it is transmitted over several networks electronically”. Additionally, “before it has to protect the data integrity, data confidentiality and availability but the mainly it protects, controls and monitors the information access. Technical security mechanisms are the term used to prevent those who are not authorized to access the data during when the data is being transmitted through network. Technical controls incorporate passwords, firewalls, network intrusion detection systems, and access control lists and data encryption. The guideline of least benefits is a specialized technical control that requires an individual, program or system process not to be allowed any more access privileges than are necessary to perform the task). 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. In this case, the activities concerning electronic patient records are followed to identify who received unveiled information. 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 (Åhlfeldt & Soderstrom 2010).

These safeguards include hardware, software, and other technology that limits access to e-PHI. These technical safeguards include: Access controls to confine access to PHI to authorized staff only review controls to monitor activity on systems containing e-PHI, such as an electronic health record system Integrity controls to avert improper e-PHI alteration or destruction. Transmission security measures to secure e-PHI when transmitted over an electronic. In 2013, Cisco reported that 99% of Android gadgets were targeted by versatile malware and 71% of Android users encountered with all forms of web-delivered malware.

In another report about cyber security trends and challenges, it was revealed that in 2014, 64% of organizations showed that their security infrastructure was continually up to date and constantly upgraded. However, in 2015, that number diminished to 59%. This proof shows that organizations are facing a greater attack surface, the growing proliferation and sophistication of attack models, and more complexity within the system. Farzandipour *et al.*, (2010) it is remarkable that security rehearses incorporate management processes for detecting and mitigating information risks as well as implementing technical safeguards. However, many healthcare organizations consider information security as a technical issue. This view must be changed to be progressively comprehensive socio-technical perspective on information security and has to emphasize the importance of integrating technical solutions with organizational security culture, policies, and education. Kwon and Johnson (2013) 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 the employees and organizations.

This study demonstrates the requirements of user identification and authentication of access control. Encryption is acquainted as a powerful and amazing tool to support the storage and transfer of data (Odabi & Oluwasegu 2011). Telemedicine gives medical care through a functioning media such as the Internet, mobile and satellite. Therefore, utilizing telemedicine gadgets largely depends on the information system security (Zaidan & Zaidan 2011).

2.5 Physical Security

Physical and administrative security controls are yet to be executed at the facility to ensure against unauthorized access and to ensure its physical trustworthiness of IT service resources at the Hospital facilities. This physical and administrative security controls include, Physical access controls, physical protection of Information Resources and environmental security.

ICT resources must be protected from any harm, unapproved access and theft, both in and out of the hospital. Any delicate information stored on removable gadgets or media must be encrypted and put in a protected area. Sensitive information that is stored outside MTRH premises must be encoded and stored in a controlled zone. Physical security controls are yet to be executed completely at all MTRH ICT facilities, including data centers, computer rooms, and work places to protect ICT assets, these controls incorporate lightening arresters, Protection against water harm from water supply lines, sewer frameworks, and rooftop leaks, temperature and dampness' shields safeguards to monitor and maintain acceptable levels. Protection against flooding, earthquakes, or other natural disasters, fire detection and suppression equipment (e.g., smoke and heat detectors, handheld fire extinguishers, fixed fire hoses, and sprinkler systems, Surge protection must be implemented for critical ICT equipment, emergency lighting systems must be implemented to illuminate emergency exits and evacuation routes in the event of a power blackout or disturbance.

Physical safeguards control access to computer systems and Facility access controls. Requirements of physical safeguards include locks and alarms, to ensure only authorized personnel have access into. 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. These safeguards are physical measures, strategies policies, and procedures that protect electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The security standards under physical safeguards include facility access controls, workstation use, workstation security, and device and media controls. The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems whether such systems are housed on the covered entity’s premises or at another location. Physical safeguard security standard is to deal with controlling physical access to protect the data against unauthorized access. 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.

2.6 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 (Appari & Johnson 2010).

Ravizza *et al.,* (2019) States that information security has been standardized and defined by WHO health informatics standards and other global standards including, ISO, more explicitly by the standard ISO/IEC 27799 on information security management and ISO 9126-1 on software quality. The standard gives guidelines for information security management and defines information security within three terms; Secrecy, Accuracy and Accessibility Secrecy deals with the idea that information should only be accessible to those with right authorization to read and utilize the information. Steps are needed to ensure that no unauthorized use happens. The accuracy of information regards protecting the information so that it is accurate, complete and correct. Therefore, information concerns ensuring that users have access to the information they need when they need it without delays.

Kruse et al., (2017) states that security standard ensures that information of health care is secure and the electronic health records are confidential. Keeping crucial information secure is imperative to all organizations. This is done by practicing information security, and the work must begin with an administration supporting the workers and also by educating end users and organization members in information security. When dealing with patient data and data related to health there are some laws and regulations healthcare providers need to abide by. The laws and guidelines can contrast among nations and this section will only focus on laws and regulations applicable to Kenya. Nevertheless, it should be noted that an enormous part can be generalized to many other countries with similar systems.

Information security management is a continuous, structured and systematic security approach to managing and protecting the organizations information from being compromised by irresponsible parties. To ensure the information remains secure many organizations have implemented information security management, in the clinical environment of a hospital is conveniently managed by utilizing EHR systems without the need for paper records. It is impossible to sufficiently protect personal medical information leakage, (Kim & Kim 2006).

Medical information systems are intended to store and share information among healthcare care providers and improve health care providers and improve work efficiency of various hospital departments, prevent medical accidents and reduce the waiting time of the patients and prevent over prescription (Lee, 2012).

To actualize an adequate information-security management system, it is first important to evaluate information security and assess its hazards, and subsequently discover appropriate measures to control risks and improve security safety ISO/IEC 27000:2009. The International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) have characterized the international standards for information and data security (ISO/IEC 2700x, Information technology – Security techniques) that are widely accepted and can be utilized to assess dimensions of security. The standards recognize three main components of information security: confidentiality, availability, and integrity. They also describe requirements for an information-security management system (ISO/IEC 27001), a code of practice (ISO/IEC 27002) (ISO/IEC 27002:2008), implementation guidelines (ISO/IEC 27003) and parameters to be measured (ISO/IEC 27004), and risk management (ISO/IEC 27005). Ravizza *et al.*, (2019).

Education is a significant component of successful management of information security and to determine appropriate actions and education efforts, chief information officers (CIOs) need to know the existing conditions in their organization and have both estimating tool and benchmark values at their disposal. However, no study has compared hospitals with respect to information security. This might be because information about the security level of an institution is delicate and might influence the hospital's perceived trustworthiness or that assessing it might itself be a security threat. The lack of an effective benchmark tool for the assessment of the status quo of information security may be another explanation for the absence of such comparisons (Glaser and Aske 2010).

Switzerland has a national execution strategy for efficient and safe eHealth systems in which, for reasons of lawful rights and adequacy, information security plays a central role. The objective of this investigation is to assess the current status of information security in Swiss hospitals. As a first step, an ISO/IEC 27002-agreeable device that allows for both a rapid nationwide assessment of hospital security and the provision of benchmark data for CIOs was developed. By utilizing this tool, the present examination aims to evaluate information security focusing on differences between hospitals of different sizes and types (private vs public hospitals and academic vs non-academic hospitals) and that there are several techniques for evaluating information security risks and most of them include recognizing threats and vulnerabilities, analyzing the likelihood and impact related with the known dangers, and ultimately, prioritizing the risks to determine the appropriate level of training and controls necessary for effective mitigation (Robert & Wilkinson (2013).

According to Cain and Mittman (2002) to be able to share health information, security across the software from multiple vendors is critical. Without security, access to data becomes difficult which in turn leads to inefficiencies, increased cost, and poor quality (Stiell, Forster, Stiell, & Van Walraven, 2003). An essential building block of information security is necessary terminology and messaging standards that are agreed upon (Brooks, 2010). Terminology standards provides an unambiguous, machine-readable meaning of specific terms and messaging standards permitting the electronic exchange of information consistently (Dlodlo & Systems, 2017). Together, they will allow the secure use and exchange of healthcare information. Miller and Sim (2004) stated that even with the wide adoption of HMIS true healthcare transformation will not occur without the standardization and improved interoperability of healthcare systems.

The IT-GrundsChutz method, which was proposed by the Federal Office for Information Security in Germany, classified the threats to five groups (force majeure, organizational shortcomings, human mistakes, technical failure and deliberate acts): In this technique, safeguard measures were infrastructure, organization, personnel, software and hardware, communication and contingency plan and the recommendations of the National Institute of Standards and Technology have been considered as a rule for a comprehensive risk assessment program.

This concerns the management of information security; strategies, policies, risk assessments etc. This is the security of any organizational level that concerns the business as a whole. It is positioned towards what the overall security requirements should be. 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 critical IT systems. Administrative is also called procedural or management controls and measures need to be put in place in terms of security policies, procedures and standard guidelines (Kaja, Anze and Igor 2020).

This study is guided by Service Oriented Architecture (SOA) theory that executes security as a service through equipment-based gateway and XML intermediary and proxy that can parse, filter, channel, validate schema, decrypt, approve signatures, access-control, transform, and sign and encode XML message flows. This security application is a server-side security portal that considers all keys and tokens used to give integrity and confidentiality to hospital services exposed through the gateway to be managed at one point. The SOA will guarantee that security requirements such as Confidentiality, Integrity, Authenticity, Authorization, Non-Repudiation and Accountability are fulfilled. The requirement of Confidentiality will be achieved through the use of an encrypted patient identifier in order to keep personal data separate from healthcare information through the secure exchange message. The solution will be provided by an access control that follows the Attribute-Based Access Control model (Remah and Khaled 2017).

Information system architecture are grouped are as follow: Hardware architecture; Software architecture and Enterprise architecture. Software architecture refers to the basic elements of a software system. It's the backbone of Information system architecture as it's concerned with how programs and application components are internally built. Hardware architecture refers to the identification of the system's physical components and how their interrelationships. It's an important component of information system architecture as it provides software designers with relevant information needed for software development and integration. Enterprise architecture on the other hand applies principles and guidelines that help organizations in business, information processing, and technological changes necessary to execute strategies (Vasconcelos, Sousa & Tribolet, 2003).

Vasconcelos et al., (2003) go further to state that Information System Architectures are usually distinguished by three aspects or sub-architectures that define the ISA functions. They are; Informational Architecture or data architecture which represents main data types that support an organization. Application Architecture defines applications needed for data management and business support, and finally, Technological Architecture that represents the main technologies utilized in application implementation and the technological infrastructure that provides an environment for Information system development.

According to Abdulla et al., (2017), the architectural design of HMIS is classified according to the number of functions that can be supported by it. HMIS systems suitable for small to medium level hospital consist of only one database that stores all patients' related data. The network architecture of such systems is client-server with a centralized database. They include one mainframe server connected to multiple terminals or workstations. In this kind of architecture, application components: patient registration; Accounting and Finance; Billing; Radiology; Pharmacy; Stores are on the framework to be accessed by the terminals.

2.7 Theoretical framework

Technical, physical and administrative security measures are required to achieve a secure Electronic Health Records system. The literatures pertaining to health system information security is also reviewed. This study is founded on Systems Theory formulated by Ludwig von Bertalanffy (1955) and Joseph Litterer (1969) the hallmarks are the interrelationship and interdependence of objects and their attributes. System Theory covers the importance of enforcing information security Technical, Administrative and physical controls in managing risks, internal process controls and information auditing. By doing so, it covers information security holistically in terms of interaction between systems, transforming systems to achieve the goal, environmental and other disorderly factors on systems, regulatory impact on systems, system hierarchies and subsystems impact on the system, differentiation among the subsystems and multiple/alternative ways to achieve system objectives (Skyttner, 2005). System theory will provide a good framework in which security policies will be developed based on authentication and authorization confined within a security model for securing Electronic Health Records for Moi Teaching and referral Hospital. System theory channels controls just like Bell Lapadula model which is referred to as “no read up, no write down” and is a formal state transition model that defines the access rules, users can only view content at or below their own security level.

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.

Information security theory is defined as a concept within a boundary set of assumptions and constrains (Bacharach, 1989). The information security goal is to ensure that confidentiality, integrity and availability of information resources (Von Solms and von Niekerk 2013).

2.8 Research Gap

Review of literature shows that a number of studies have been carried out on information security in healthcare in terms of damages caused by information security. Very little has been done on information security models for electronic health records that provide rules for technical security in terms of detection systems, data encryption and access to the system. Unrestricted USB drives open wireless network settings by use of default routers. This allows experienced hackers to access IP addresses. There is also a research gap on internet outage communication protocol and communication process. The need to have physical security measures considered, this includes installing fire extinguishers in place.

2.8.1 Conceptual Framework

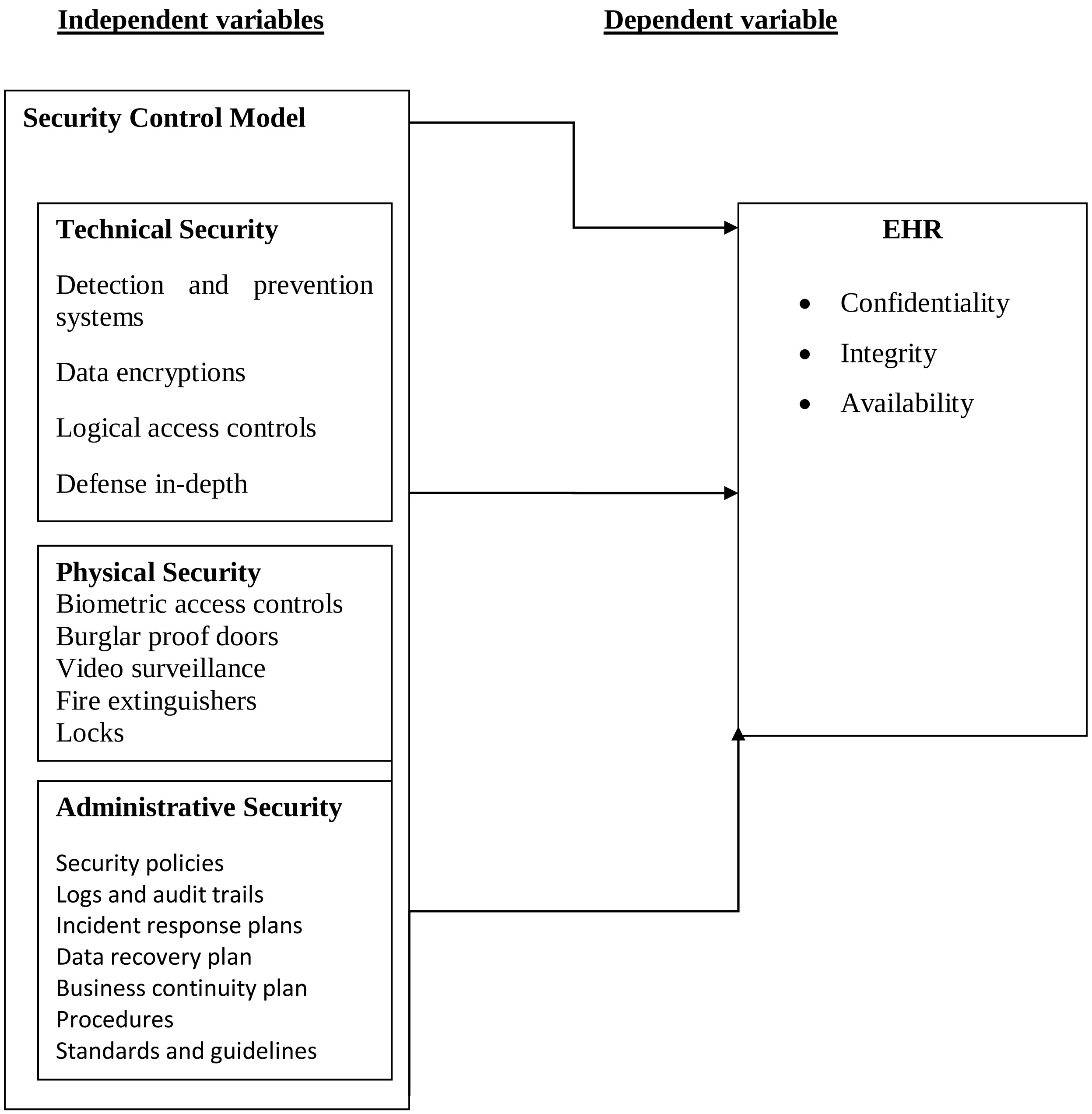


Figure 2. 1: Conceptual Framework

Source: Researcher (2020).

The conceptual framework shows the relationship between the independent and depended variable on the security of the electronic health records systems. The independent variable influences the dependent variable to have an outcome of a secure EHR. This occurs through the interrelationship and interdependence of the three security controls. The independent variables provide a number of security layers of the security control model represented by the technical, physical and Administrative security controls that ensures that the dependent variable is outcome is a secure EHR.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Research Design

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 (Bryman & Bell 2011).

3.2 Study Area

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. With the large number of patients in MTRH, the hospital has big data that needs to be secured.

3.3 Target population

The target population was the MTRH health record staff working in the eight departments. The hospital has a total of 200 health records staff members as indicated in **Table 1** below. This is as per the MTRH human resource office (2019).

Table 3. 1: Sample Frame.

Health Records Department	**Number of Staff**	**Sample Size**
OPD	**64**	**41**
Central Records	**25**	**17**
Shoe for Africa	**15**	**10**
Chandaria Cancer Centre	**13**	**9**
Private wing	**14**	**9**
General wards	**16**	**10**
Diagnostics Services	**42**	**29**
Mother and baby	**11**	**8**
TOTAL	**200**	**133**

3.3.1 Inclusion criteria

All records staff from eight departments were considered.

3.3.2 Exclusion criteria

- Records staff that were on leave were left out.
- Other members of staff not handling patient's health records

3.4 sample size and Sampling procedures

The sample size was determined by the using Yamane (1967) formula;

In order to obtain the subjects for the sample for the eight departments, Yamane’s formula for calculating the sample size, Yamane (1967) was used. This was a simplified formula in calculating the sample size.

$n=N/ [1+N (e)^{2}]$

Where:

n= Sample size

N=Population size

E=Sampling error (usually 0.05)

The total population is 200

$n = 200/ 1+ 200(0.05) 2$

$n = 200/ 1 +200 (0.0025000000000000005)$

$n = 200/ 1+0.5000000000000001)$

$n =200/1.5$

$n =133.33$

The above formula was chosen because it fits in situations for analyzing samples from the eight departments.

Thus, desired sample size = 133

This study used a random sampling technique. The samples were selected from eight departments dealing with patient’s health records data.

3.5 Research instruments and data collection procedures

The researcher used a questionnaire to collect data from the respondents of the aforementioned eight departments. The heads of the departments were notified and upon consent, the research instruments were then dispatched to the respondents by the researcher.

3.6 Pilot study

Test re-test method was used to pilot the research instrument prior to the main study. The research instrument was administered by the researcher to a group of respondents with similar characteristics as the final respondents, for purposes of checking if the results given by the respondents were consistent, and also checks for ambiguous questions. Respondents used in the pilot study were not included in the final study. Based on Gay (1992) and Mugenda and Mugenda, (2003), Recommendation that a minimum sample of 10-20% is adequate for educational research of less than a thousand participants, 6 respondents were used for piloting the instrument. Once the researcher was satisfied with the results that the instrument was relaying then they proceeded to use it for the actual study.

3.7 Instrumentation

The data was collected using questionnaires, which were administered by the researcher. The questionnaires which sought to answer questions related the objectives of the study. The questionnaires were administered to all the eight health records departments across MTRH using the “drop and pick” later method.

3.7.2 Reliability and validity

To ensure the reliability of the questionnaires, a pilot study was carried out first before administering all the research questionnaires. Six questionnaires were administered to outpatient department, the results showed that there was consistency when the study was repeated. This was to ensure that the items are reliable before the questionnaires were developed for the study. Reliability analysis was further determined using Cronbach's Alpha which was used as a measure of the internal consistency and reliability of an instrument. It measures how well a set of variables or items measures a single, unidimensional latent construct (Cronbach, 1951). Cronbach's Alpha is therefore not a statistical test but a coefficient of reliability or consistency. If the inter item correlations are high, then there is evidence that the items are measuring the same underlying construct. In order to ascertain this Cronbach's Alpha is computed for all the 49 items in the questionnaire. Reliability and validity coefficient of 0.70 or 70% and above is considered acceptable. The pilot study that the Cronbach Alpha values for the security of EHR under investigation were reliable and therefore the 49 items were acceptable and there was no need to delete any item.

3.8 Data Analysis and Presentation

The data collected from research instrument was coded and analyzed using Statistical Package for Social Sciences (SPSS) version 22.0. The results obtained were presented in form of descriptive statistics comprising of frequency tables and charts. More specifically, data was segregated according to the three specific research objectives to ease analysis and ultimately the respective findings aided the researcher in designing a security control model for Electronic Health Records (EHR) at MTRH.

3.9 Ethical considerations

The researchers applied and obtained ethical clearance from the National Commission for Science, Technology and Innovation (NACOSTI) and the Institutional Research Ethics

Committee (IREC) of MTRH to carry out this study. There principal investigator was able to seek consent from the respondents and the participation of this study was voluntary no member of staff was coerced to answer any questions. The entire process was confidential to protect the respondent's identities.

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSIONS

4.1 Introduction

In this chapter, a total of 133 questionnaires was administered by the researcher to the respondents in health records departments across MTRH. Of the questionnaires 97 were returned for analysis. The returned questionnaires accounted for 72.9% response rate. According to Mugenda and mugenda (2003), a response rate of below 40% is unreliable, a response rate of 40% - 50% is poor, 50% - 60% is acceptable for analysis reporting, above 60% is good and 70% and above is rated very well. Therefore, the response rate of 72.9.0% was acceptable.

4.2 Demographic Characteristics of Respondents

The study considered gender, education level, age, department and working experience as demographic factors that were considered because it determined that the respondents represented in the study are a representative sample of the target population.

4.2.1 Distribution of Respondents by Gender

The study sought to establish the gender of the respondents. Majority of the respondents were female at 62.9% while 37.1% were male. This is represented by **table 4.1** below.

Table 4. 1: presents the findings by gender

Description		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	36	37.1	37.1	37.1
	Female	61	62.9	62.9	100.0
	Total	97	100.0	100.0	

4.2.2 Distribution of respondents by Age

The study sought to establish the respondents age. From the findings the study showed that the respondent's age was between 20 years and 60 years. Majority of the respondents were aged between 31 and 40 years at 61%. This showered that they were old enough to answer the questions diligently. The figure below presents the findings

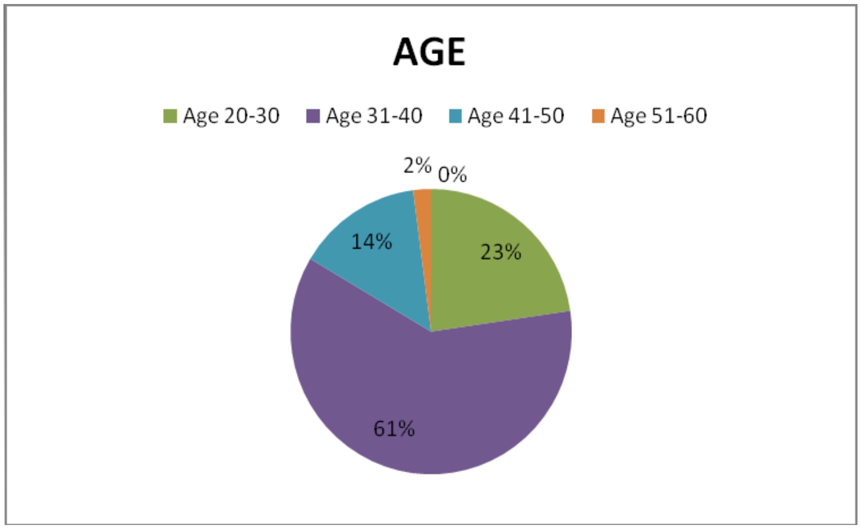


Figure 4. 1:Age

4.2.3 Distribution of respondents by the level of education.

The study sought to establish the respondents by the level of education. From the findings majority of the respondents had attained Diploma (55%), while 30 % had undergraduate degree, 13% were certificate holders and the remaining 2% were postgraduate graduates. This shows that the respondents were well educated and in position to answer the questions well. The figure below presents the findings

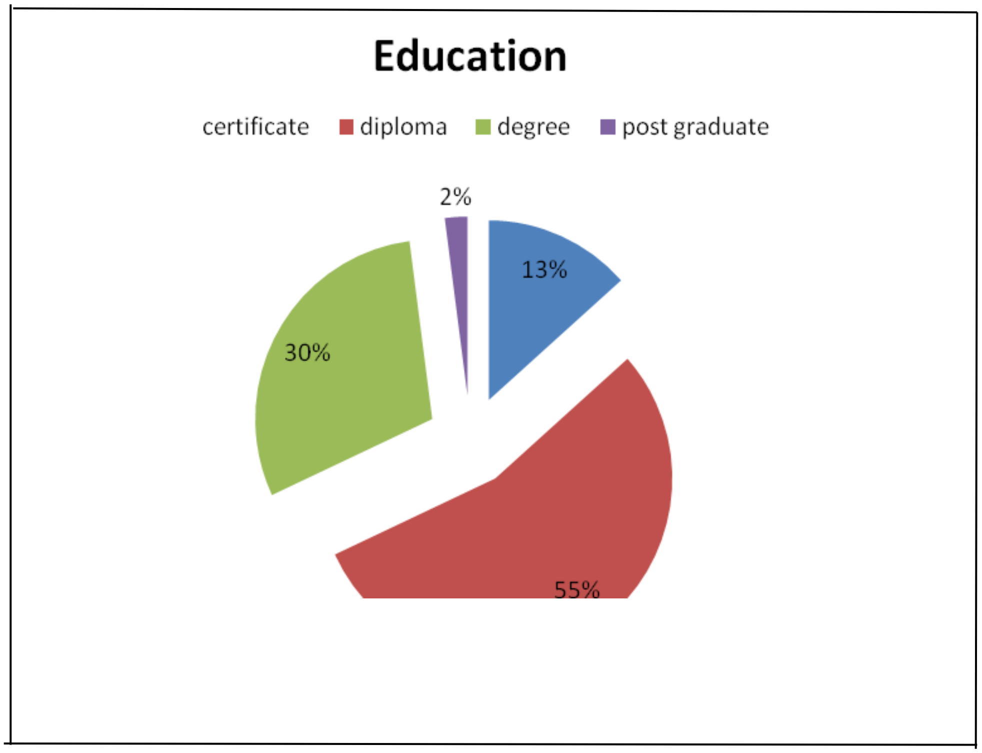


Figure 4. 2: Level of Education

4.2.4 Distribution of respondents by the department

The study sought to establish the respondents by the departments. The findings show that majority of the respondents at 22% were working OPD's ,18% of the respondents were working in the private wing department, 17% were in central records, 11% were in mother and baby, 11% in diagnostic services, 11% in chandaria cancer centre and 5.2% in shoe for Africa department. This depicts that the respondents were fairly selected to represent each department. The figure below presents the findings

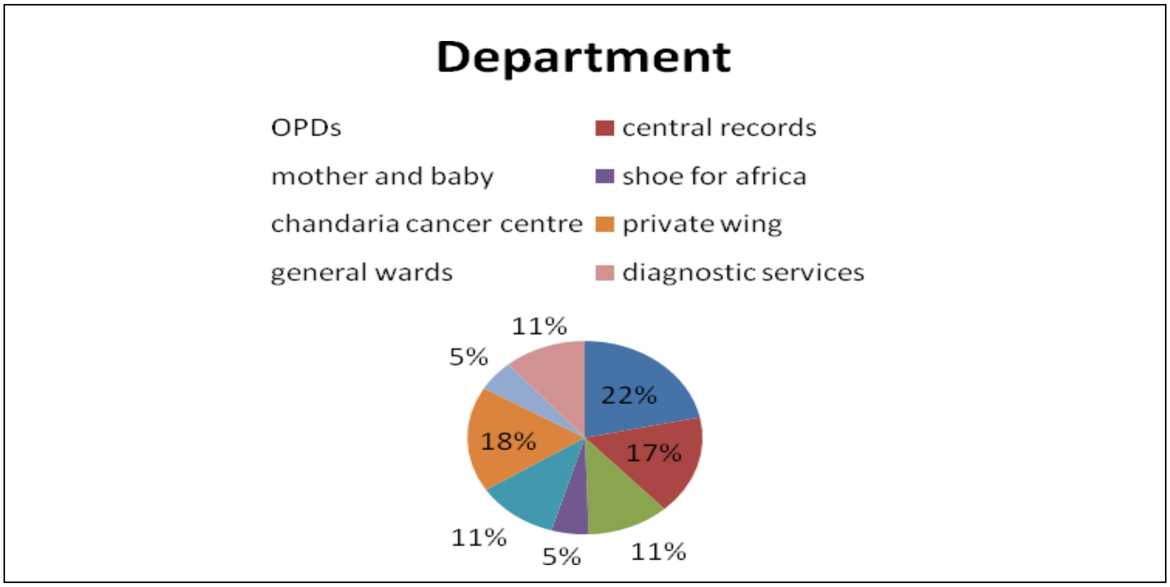


Figure 4. 3: Department

4.2.5 Distribution of respondents by Experience

The study sought to establish the respondents by their experience. From the from the findings 50.5% of the respondents indicated that they have been working in the organization for 6-10 years while 29.9% have been working for more than 10 years, 17.5% had worked for 1 to 5 years and 2.1 % had worked for less than a year. This indicates that majority of the respondents had worked in the hospital long enough, understood the hospital system well and were in a good position to provide reliable information. The figure below presents the findings.0

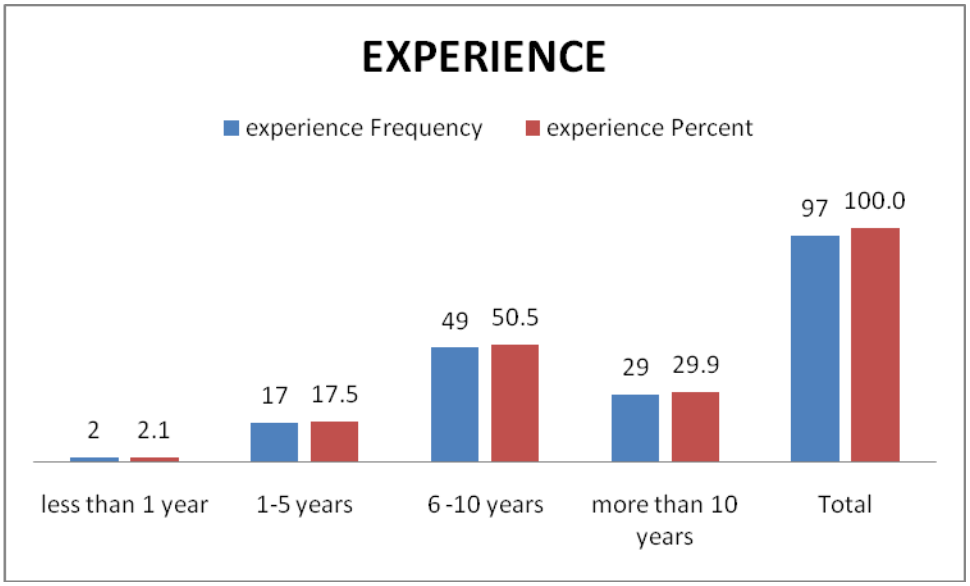


Figure 4. 4: Work Experience

The implication of the demography in study on gender shows that females and males differ in their attitudes towards information privacy towards information privacy concerns. Females are often more concerns about controls of personal information to their privacy than males.

The older users are more concerned about more concerned about online information privacy, their greater desire to control the amount of information collected about them as well, older users are sensitive to privacy issues compared to younger users (Kaja, Anze & Igor 2020).

4.3 Current Security controls for EHR

This section analyzed data on the current controls for the Electronic Health Records in MTRH by looking at the Technical Security Controls, Physical Security Controls and the Administrative Security Controls.

4.3.1 Technical Security Controls

The respondents were asked to indicate the extend to which the current Technical security controls were applied in the hospitals EHR system. Table 4.2 shows the findings.

Table 4. 2: Technical security Control

Indicator	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree	TOTAL
There is a good antivirus protection that is designed to monitor computer systems and identify computer viruses or malware in real time	0 0.0%	48 49.5%	17 17.5%	30 30.9%	2 2.1%	97 100.0%
The antivirus is updated frequently to keep pace with new viruses.	0 0.0%	71 73.2%	20 20.6%	6 6.2%	0 0.0%	97 100.0%
The hospital has ensured that all the computers have passwords for protection of data.	0 0.0%	2 2.1%	2 2.1%	5 5.2%	88 90.7%	97 100.0%
MTRH ensures that sensitive information is protected and only authorized personnel have access	0 0.0%	2 2.1%	0 0.0%	6 6.2%	89 92.8%	97 100.0%
The hospital ensures that passwords are changed in periodic basis	40 41.2%	2 2.1%	3 3.1%	50 51.5%	2 2.1%	97 100.0%
The health providers have access to patient information when needed.	0 0.0%	3 3.1%	5 5.2%	62 63.9%	27 27.8%	97 100.0%
The hospital ensures that the medical records are protected against distortion.	11 11.3%	16 16.5%	9 9.3%	61 62.9%	0 0.0%	97 100.0%

49.5% of the respondents disagreed that the computer systems had a good antivirus protection to counter the numerous viruses and malware in real time. Majority of the respondents also disagreed that the antivirus was always up to date. On the other hand, majority of them agreed (90.7%) that sensitive information is protected and only authorized persons have access. This finding shows that there is a greater and better access to patient records (Alotaibi & Federico 2017), therefore there will be an easier control of patient’s health information (Sotto *et al.*, 2010), making Electronic health records systems an environment that is safe.

This shows that the current Technical security controls are in place to secure the Electronic Health Records. Unfortunately, a bigger percentage seem not to agree with the majority, therefore the hospital should look into all the departments to ensure that the technical controls are all in place.

4.3.2 Physical Security Controls

The respondents were asked to indicate the extend in which the current Physical security controls were applied in the hospitals EHR system. **Table 4.3** presents the findings.

Table 4. 3: Physical Security Controls

Indicator	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree	TOTAL
The hospital has ensured that the rooms and cabinets with patients' information are under lock and key to avoid unauthorized entry	2	2	0	25	68	97
	2.2%	2.1%	0.0%	25.8%	70.1%	100.0%
The motion detection systems are in place to detect any motion from potential intruders and raise the alarm	4	31	16	32	14	97
	4.1%	32.0%	16.5%	33.0%	14.4%	100.0%
The hospital has a closed-circuit Television (CCTV)system in place to record and detect any occurrence	0	15	5	59	18	97
	0.0%	15.5%	5.2%	60.8%	18.6%	100.0%
MTRH ensures that terminated or transferred employees access codes are terminated in a timely manner	1	9	7	74	6	97
	1.0%	9.3%	7.2%	76.3%	6.2%	100.0%
The hospital has door alarms to detect any unauthorized persons accessing the building	11	6	4	62	14	97
	11.3%	6.2%	4.1%	63.9%	14.4%	100.0%
The hospital ensures that individuals wishing to access the records departments obtain identifications before entry	0	4	7	71	15	97
	0.0%	4.1%	7.2%	73.2%	15.5%	100.0%

The findings on the current Physical security controls showered that majority of the respondents (70.1%) strongly agreed that the hospital ensured that the rooms and cabinets with patient's information were under lock and key. Ayatollahi and shagerdi (2017), states that requirements of physical security should include locks, alarms to ensure only authorized personnel have access the facility that house that house the data and the system. Majority of respondents further agreed that most of the controls were in place, this includes CCTV system (60.8%), access codes for terminated or transferred members of staff were terminated in a timely manner (76%), door alarms were in place (76%), unauthorized persons wanting to access the building obtain identification before entry (73.2%) and on motion detection systems (33%) agreed that they were in place while (32%) disagreed. This shows that either half of the respondents did not know what the motion detectors are or all of them had no idea and had never seen it. (Robert & Wilkinson, 2013)) states that the physical dangers to information security occurs when internal and external agents access the patient’s information leading to misuse of data. Therefore, internal threats can be controlled physically, Ray and Newell (2010).

4.3.3 Administrative Security Controls.

The respondents were asked to indicate the extend in which the current Administrative security controls were applied in the hospitals EHR system. **Table 4.4** presents the findings.

Table 4. 4: Administrative Security Controls

Indicator	Strongly Disagree	Disagree	Uncertain	Agree	Strongly agree	TOTAL
The hospital ensures accuracy of medical records by protecting the information against losses	0	2	5	75	15	97
	0.0%	2.1%	5.2%	77.3%	15.5%	100.0%
The hospital has ensured that issues of information security issues are addressed promptly	0	0	6	76	15	97
	0.0%	0.0%	6.2%	78.4%	15.5%	100.0%
Health records are handled by qualified personnel only?	2	2	3	60	30	97
	2.1%	2.1%	3.1%	61.9%	30.9%	100.0%
The hospital ensures healthcare providers only discuss a patient in need	1	12	7	69	8	97
	1.0%	12.4%	7.2%	71.1%	8.2%	100.0%
The hospital ensures that information security training takes place frequently.	5	31	11	44	6	97
	5.2%	32.0%	11.3%	45.4%	6.2%	100.0%
The hospital ensures that the user is only provided with necessary information	0	3	3	45	46	97
	0.0%	3.1%	3.1%	46.4%	47.4%	100.0%
The hospital has ensured that all the employees have knowledge of information security policies and guidelines	2	0	2	65	28	97
	2.1%	0.0%	2.1%	67.0%	28.9%	100.0%
The hospital ensures that employees handling patients records have IT knowledge to key in accurate data into the system	1	2	2	70	22	97
	1.0%	2.1%	2.1%	72.2%	22.7%	100.0%

According to the study findings, majority of the respondents agreed that the hospital ensures accuracy of medical records (77.3%), it also shows that MTRH has ensured that information security issues are addressed promptly (78%%), majority of the respondents were in view that information security trainings takes place frequently (45.4%) while 32% of the respondents disagreed that information security trainings takes places frequently. This shows that the hospital has not ensured that all employees are trained equally on issues of information security. The hospital has ensured that all the employee have knowledge of information security policies and guidelines 67% of the respondents agreed while 28.9 % strongly agreed 61.9% of the respondents agreed while 30.9% strongly agreed that the health records was handled by qualified personnel. 71.1% of the respondents agreed that the hospital ensured that the healthcare providers only discuss the patients in need and that a user is only provided with necessary information, 47% strongly agreed and 46% agreed and because security and protection are specific therefore privacy is handling policy, but security is managing the tools to implement the policy (Lu *et al* (2013). This indicates that the hospital has a good administrative security controls therefore the information is well guarded and is available to only authorized personnel therefore ensuring that there is integrity.

4.4 EHR Security Controls Requirements

This section analyzed the Electronic Health Records security control requirements on Technical, Physical and Administrative security controls.

4.4.1 Technical Security Controls

The respondents were asked to indicate their priority on the Electronic Health Records security control based on Technical security controls. **Table 4.5.** presents the findings.

Table 4. 5: Priority requirements on Technical Security Control

Indicator	Strongly Disagree	Disagree	Uncertain	Agree	Strongly agree	Agree-Disagree	Rank%
The hospital ensures that Health records are backed up regularly to prevent loss of data.	0.0%	2.1%	6.2%	60.8%	30.9%	91-2.1 =88	88.00 %
The Smoke sensors and heat sensors are in place	15.5%	71.1%	10.3%	3.1%	0.0%	3.1- 86.5=83. 5	-83.5%
Intrusion Detection System software application and devices are in place to monitor computer systems for malicious activity	6.2%	55.7%	2.1%	36.1%	0.0%	36.1- 61.7 = - 25.6%	- 25.00 %
There are system and network monitoring tools used to record log-ins and access to particular application to prevent unauthorized users.	4.1%	54.6%	4.1%	35.1%	2.1%	37.2- 58.7 = 21.5	-21.50 %
There is firewall that blocks any unauthorized activity within the system	23.7%	60.8%	6.2%	8.2%	1.0%	9.2- 83.5= 75.3	-75.00 %
The hospital wireless network is encrypted so that unauthorized person doesn't understand	4.1%	10.3%	6.2%	44.3%	35.1%	79.4- 14.3 = 65.0	65.00 %
The network being used by staff handling patient health records is isolated from the network being used by other members	7.2%	53.6%	7.2%	29.9%	2.1%	32-60.8= -28	-28.00 %

60.8% of the respondents agreed while 30.9% strongly agreed that the hospital ensures that the health records data is backed up regularly. 70.1% of the respondents agreed while 19.6% strongly agreed that the user rights were reviewed frequently. The respondents further disagreed that the smoke sensors and heat sensors were in place at 71.1% while 10.3% were uncertain.55.7% disagreed while 36.1% agreed that intrusion detection systems software application and devices were in place to monitor any malicious activities, this shows that a good number of the respondents had no idea what the intrusion system is therefore could not give a clear feedback. 54.6% of the respondents disagreed and 35.1% strongly disagreed that the hospital has ensured that there are Log-INS and access to particular applications to prevent any unauthorized user. Majority of the respondents also disagreed 60.8% and 23.7% strongly disagreed that firewall is installed to block any unauthorized activity within the system. 44.3% agreed and 35.1% strongly agreed that the hospital network has been encrypted so that unauthorized users don’t understand the information. 53.6% disagree and 29.9% agree 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 patients 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. (Datta & Banerjee 2010). Technical controls also help in detecting and mitigating information risks, Farzandipour *et al.,* (2010). This study shows that the intrusion and detection systems are not installed in the hospital. The respondents also indicated that system monitoring tools used to record log-ins to prevent unauthorized access is also not in place. The EHR system is at risk at the MTRH, the respondents stated that there is an absence of a firewall that blocks any unauthorized activity within the system.

This depicts that the technical security requirements need to be put in place to protect patient's information by integrating solution with security culture and education (Kwon and Johnson,2013).

4.3.4 Physical Security Controls

The respondents were asked to indicate the extend of the Electronic Health Records security control requirements on Physical security controls. Table **4.6** presents the findings.

Table 4. 6: Priority requirements for Physical Security Controls

Indicator	Strongly disagree	Disagree	Uncertain	Agree	S. Agree	Agree/disagree	Rank%
Power generators installed in the hospital in case of electricity failure	0.0%	0.0%	0.0%	6.3%	93.8 %	100.00- 0.00	100.00 %
Fire extinguishers are installed in rooms with patient's information	0.0%	23.7%	12.4%	22.7 %	41.2 %	63.9 – 23.7= 40.3	40.3 %
Fire sprinklers have bee In case of fire outbreak	9.3%	74.2%	9.3%	4.1%	3.1%	-7.2- 83.5= 73.9	-73.9 %
Uninterruptable power : Records section for po	5.2%	68.0%	4.1%	22.7 %	0.0%	-22.7– 73.2=	-50.5%
Rooms with patient's information are fireproof and secure	23.7%	68.0%	6.2%	2.1%	0 0.0%	-2.1- 91.7	-89.6%
There is a monitoring station within the hospital to monitor daily occurrence.	2.1%	51.5%	8.2%	36.1 %	2.1%	-38.1- 53.6	-15.5%
Temperature controls and dedicated air conditioning are in place	19.6%	63.9%	6.2%	8.2%	2.1%	-10.3 - 83.5	-73.2%

Nearly all 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. Majority disagreed at 74.2% that fire sprinklers were installed at the health records section to put out fire in case fire breaks out. 41.2% strongly agree, 22.7% agree and 23.7% disagree that fire extinguishers are installed in case of fire. 68.0% disagree while 22.7% agree that the uninterruptable power supply was installed at the health records section. 68.0% of the respondents. 68% of the respondents disagreed that rooms with patient information are fireproof and not secure while 23.7% strongly disagreed. Temperature controls and air conditioning in place, 63.9% disagree and 19.6% strongly disagree.51.5% disagree, while 36.1% agree that there is a monitoring station at the hospital to monitor the daily occurrence, Therefore, this study advice on good physical security controls to be installed in place to secure patients information.

4.3.5 Administrative Security Control

The respondents were asked to indicate the extend of the Electronic Health Records security control requirements on Administrative security controls. Table **4.7** presents the findings.

Table 4. 7: Priority requirements for Administrative Security Controls.

Indicator	Strongly disagreed	Disagree	Uncertain	Agree	Strongly agree	Agree/Disagree	Rank %
Reports are reviewed regularly by the Chief Information security Officer	0.0%	0.0%	1.0%	58.8%	40.2%	99.0-1.0= 98.0	98.0%
There is a computer incident response team in place in case of the system failure	0.0%	27.8%	10.3%	47.4%	14.4%	53.0-27.8=45.2	45.2%
The hospital has developed a plan of action and milestones for a continuous monitoring.	0.0%	36.1%	26.8%	34.0%	3.1%	37.1-36.1 =1.0	1.00%
The hospital management has developed and published a written access control policy on information security	2.1%	44.3%	13.4%	37.1%	3.1%	-40.2-46.4= 6.2	6.2%
There are procedures for removing access rights.	0.0%	0.0%	2.1%	64.9%	33.0%	97.9-0.0= 97.9	97.9%
The hospital has written procedures for the creation (registration) and deletion (deregistration) for user accounts.	0.0%	5.2%	5.2%	75.3%	14.4%	89.7-9.3= 80.4	80.4%
When a new account is created, the user is required to change to his/her password conforming to the hospital policy	0.0%	9.3%	5.2%	69.1%	16.5%	83.6-9.3= 74.3	74.3%
There are Procedures related to the security controls over access to the system	1.0%	3.1%	15.5%	63.9%	16.5%	80.4-4.1= 76.3	76.3%

The respondents strongly agreed (40.2%), 14.4% agreed that the reports are reviewed regularly by the Chief Information Security Officer while 27.8% disagreed. 47.4% of the respondents agreed that there is a computer incident response team in place in case of the system failure, 27.8% disagreed. The hospital has developed a plan of action and milestones for a continuous monitoring, identifying and addressing the systems weakness in security implementation, 36.1% of the respondents disagree, 34.0% agree and 26.8% were uncertain. 44.3% disagreed that the hospital management has developed and published a written access control policy on information security, 37.1% agreed while 14.4% were uncertain. The respondents further agreed that there are procedures for removing access rights for a terminated employee, 64.9% agreed and 33.0% strongly agreed. The respondents further agreed at 75.3% and 14.4% agreed that the hospital has written procedures for creation and deletion of user accounts. 60.8% of the respondents agreed that users are required to sign access agreement while 26.8% disagreed. Default passwords for the system devices or application are allowed anywhere in the hospital 52.6% disagree, 20.6% agree. There is a developed and written policy on the use of network services within the hospital 45.4% disagree and 35.1% agreed. 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.

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 (Samabeik et al., (2015).

This shows 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 were existing procedures and policies that guarantee information confidentiality, availability and integrity.

4.4 Model a security control model for EHR system

This study modelled 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.

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 showed 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.

4.4 Security Control Model

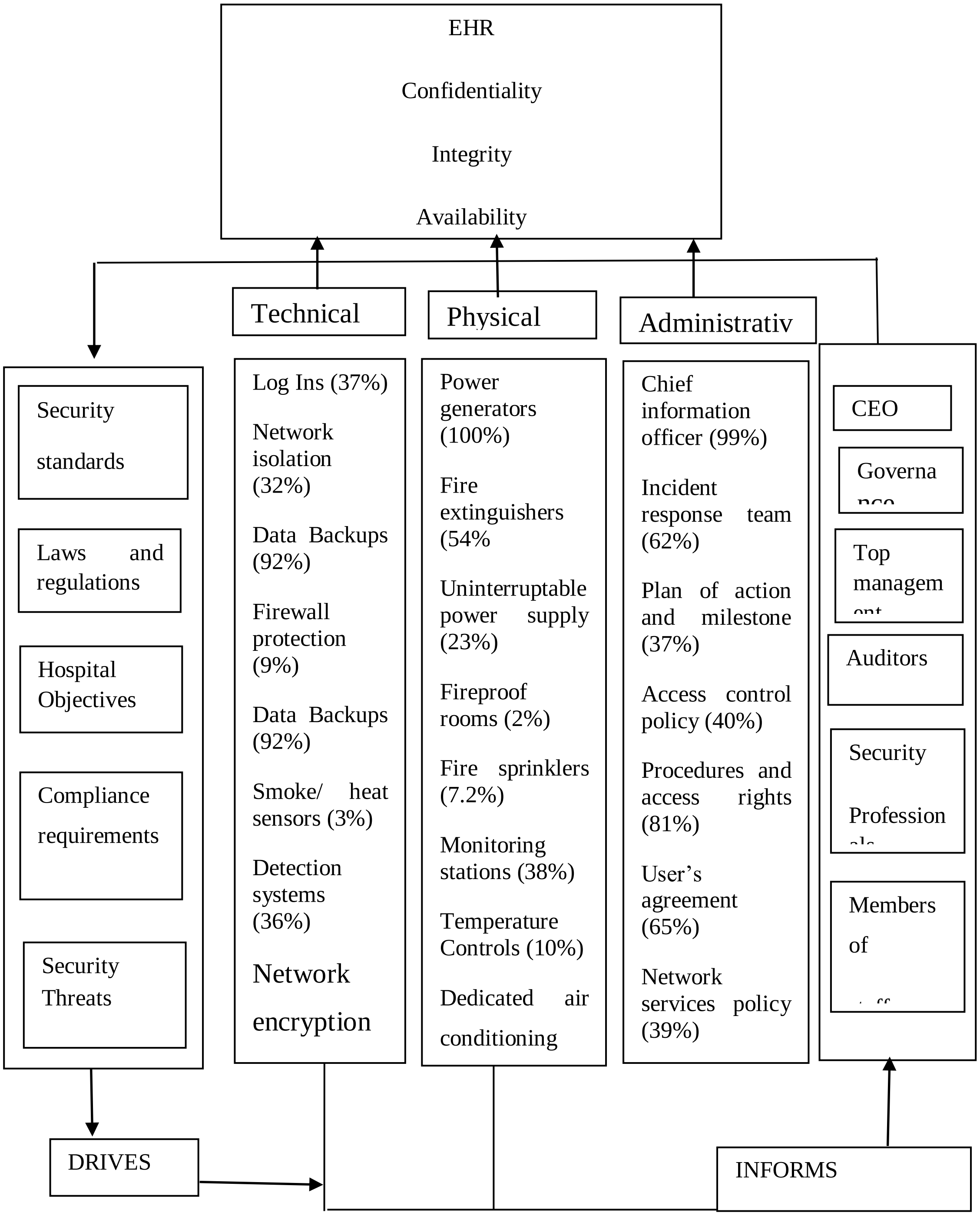


Figure 4. 5: Security Control Model

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.

CHAPTER FIVE: SUMMARY OF THE FINDINGS, CONCLUSION AND RECOMMENDATION

5.1 INTRODUCTION

This chapter presents the summary of the study and gives conclusion and recommendation drawn from the findings in chapter four.

5.2. Security controls of the Current Electronic Health Records system

The study sought to examine security controls of the current electronic health record system at the Moi Teaching and Referral Hospital. The study revealed that most respondents agreed that most of the current technical security controls are in place. The respondents to a larger extend agreed that there was a good antivirus designed to deal with viruses and malware but they disagreed that the antivirus was not updated regularly. Further the respondents agreed that MTRH ensures that sensitive information is protected and only authorized persons access the information and that the data was encrypted so that unauthorized parties cannot understand the information. They went ahead and agreed that the healthcare providers have access to patient information when needed and that the hospital ensures that medical records are protected while being transmitted through the electronic media. Odabi & Oluwasegu (2011) states that Encryption is acquainted as a powerful and amazing tool to support the storage and transfer of data.

On physical security controls the respondents agreed that the hospital ensures that the rooms and cabinets with patient information are under lock and key. They also strongly agreed that the motion detection systems and CCTV cameras are installed at the health records departments. They further agreed that the door alarms were installed and individuals wishing to access the health records department obtain identification before entry.

The respondents agreed that the hospital ensures that the information security issues are addressed on time and the health records are handled by qualified personnel and the health providers only discuss a patient in need. Majority of the respondents stated that the hospital ensures that the information security trainings takes place frequently and that staff have knowledge of information security policies. This shows that the current security controls in MTRH are in place. Therefore, there is confidentiality, integrity and availability of patient's information.

Dupler (2011), states that information security 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.

5.2.3 Security Control requirements for MTRH

The study findings on the technical security control shows that the respondents agreed that the hospital ensures that health records are backed up regularly, they also agreed that the hospital wireless network is encrypted so that unauthorized users don't understand the information. Majority of the respondents highly disagreed that smoke sensors and heat sensors are not in the records department. They further disagreed that the intrusion and detection system software application and devices are in place to monitor the computer systems and network monitoring tools used to record log-ins to prevent unauthorized persons. The finding also shows that the firewall has not been installed to block any unauthorized activity within the system. The network being used by records staff is not isolated from the network being used by other members of staff.

The findings of the physical security control requirements for MTRH majority of the respondents strongly agreed that the hospital had installed generators in case of power failure and that the fire extinguishers had also been installed at the health records department. Majority of the respondents however strongly disagreed that fire sprinklers were installed in the health records departments in case of fire outbreak. They further disagreed that the uninterruptable power supply for power back. The rooms with patient information are not fire proof and no temperature controls and dedicated air conditioning in place. The respondents went ahead and stated that the hospital has no monitoring station within the hospital to monitor any unauthorized activity within the hospital.

The administrative security control requirements findings show majority of the respondents agreed that the information reports were reviewed regularly by the chief information security officer, and that there was a computer incident response team in case of system failure. The respondents further agreed that the hospital had developed, published and written policies on information security, information security audits are done frequently, and there are procedures for removing access rights for terminated employees and unauthorized users. The respondents disagreed on two administrative security control requirements, the plan of action and milestones for continuous, monitoring, identifying the system weakness in the security control implementation and that the hospital has not developed and written any policy on the use of network services in the hospital.

5.2.4 Security control model for Electronic Health records.

The recommended model will ensure that the EHR system outcome is confidentiality, integrity and availability. This is represented by the three security controls in equal measures, Technical, physical and administrative controls. The three security controls will contribute to information security equal. They will all work hand in hand to protect patient information. This is derived from three models; the Clarkson-Wilson model that focuses on integrity of data, Bell-Lapadula model that ensures the information flows and is confidentially focused and Harrison –Ruzzo- Ullman model that ensures finite procedures are available to authorized subjects.

5.2.4 Conclusion of the study

From the findings the current security controls for the electronic health record system are positively in place, Technical security controls (40%), shows that computers have passwords; sensitive information is protected from unauthorized persons. The physical security controls (63%), installed motion detection systems and CCTV camera’s in the hospital and the doors are fitted with alarms to alert in case of unauthorized entry. The administrative security controls (69%), shows that the hospital has developed and published information security procedures, policies and the staffs are trained on information security frequently.

To establish the security controls for MTRH, showed that the administrative security controls are place and contributes more to information security (60%), unlike technical security Controls (36%) and Physical security control (36%) 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. The research showed that more technical security controls should be installed in the health records departments, such controls include; intrusion detection systems software installation, there should be a system and network monitoring tools to record log-INS and access to prevent unauthorized users. Firewall should be installed to block any unauthorized activity within a system and the network used by the health records staff should be isolated from the network being used by other members of staff. Physical security controls such as fire sprinklers, uninterruptable power supply, rooms with patient information should be fireproof; there should be a monitoring station within the hospital to monitor daily occurrences. Temperature controls and air conditioning should also be installed.

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.

This research found out that for the Electronic Health Records to be protected all the three security controls should be in place. This will promote confidentiality, integrity and availability.

5.2.5 Recommendation 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, they 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.

5.2.6 Suggestions for Further Studies

This study focused on MTRH and Since HMIS is gaining ground there is need evaluate all EHR systems and access across the country. Further research can extend their focus on how to link up and integrate EHR systems in all the public hospitals in Kenya while focusing on the security of Patient information.

REFERENCES

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.

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*.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Andriole K. P. (2014). Security of electronic medical information and patient privacy: what you need to know. Journal of the American College of Radiology: JACR, 11(12 Pt B), 1212–1216

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.

Alshinina, R., & Elleithy, K. (2017). Performance and Challenges of Service-Oriented Architecture for Wireless Sensor Networks. *Sensors (Basel, Switzerland)*, *17*(3), 536.

Alotaibi, Y. K., & Federico, F. (2017). The impact of health information technology on patient safety. Saudi medical journal, 38(12), 1173–1180.

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth Cloud Security Challenges: A Survey. Journal of healthcare engineering, 2019, 7516035.

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.

Bakhtiyari-Shahri, A., & Ismail, Z. (2011). Users as the biggest threats to security of Health Information Systems. *International Journal of Communications and Information Technology*, *1*(2), 29-33.

Brumen, B., & Makari, T. (2017, May). Resilience of students' passwords against attacks. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1275-1279). IEEE.

Bryman, A &Bell, E. (2011). Business research methods. 3rd ed. Cambridge; New York, NY: Oxford University Press.

Burrell, I. (2011). Millions of medical records lost by the NHS. *The Independent, July, 1.*

Büyüközkan, G., Çifçi, G., & Güleryüz, S. (2011). Strategic analysis of healthcare service quality using fuzzy AHP methodology. *Expert systems with applications*, *38*(8), 9407-9424.

Chen, C. Y., Hsu, Y. C., Lin, C. C., Hajiyev, J., Su, C. R., & Tseng, C. H. (2019). Study of Out-Of-Hospital Access to HIS System: A Security Perspective. Sensors (Basel, Switzerland), 19(11), 2628.

Christiansen, M. B., & Nøhr, C. (2011). Undersøgelse af klinisk anvendelse af sundheds-it-systemer 2011. *Available from: Virtuelt Center for Sundhedsinformatik, Aalborg University*.

Chukkapalli, S. S. L., Mittal, S., Gupta, M., Abdelsalam, M., Joshi, A., Sandhu, R., & Joshi, K. (2020). Ontologies and artificial intelligence systems for the cooperative smart farming ecosystem. IEEE Access, 8, 164045-164064.

Datta, S. P., & Banerjee, P. (2010). Risk management process for information security system. *Int J Comput Sci Com*, *1*(1), 33-38.

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.

Fernandes, Diogo & Soares, Liliana & Gomes, João & Freire, Mario & Inácio, Pedro. (2013). Security Issues in Cloud Environments - A Survey. Int. J. Inf. Secur.: Security in Cloud Computing. 10.1007/s10207-013-0208-7.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics*, *46*(3), 541-562.

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.

Glaser, J., & Aske, J. (2010). Healthcare IT trends raise bar for information security. *Healthcare financial management*, *64*(7), 40-45.

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

Jeddi, F. R., Hajbaghery, M. A., Akbari, H., & Esmaili, S. (2016). Technological feasibility of a nursing clinical information system. *Electronic physician*, *8*(9), 2942.

Jeffrey Daigrepont, E. F. M. P. (2011). Complete guide and toolkit to successful EHR adoption. HIMSS.

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

Kenya Government, ministry of Health (2012). The Kenya Health Sector Strategic and Investment Plan-KHSSP 2012-2017, Afya house: ministry of health.

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

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security Techniques for the Electronic Health Records. Journal of medical systems, 41(8), 127.

Kushniruk, Andre & Beuscart-Zéphir, Marie-Catherine & Grzes, Alexis & Borycki, Elizabeth & Watbled, Ludivine & Kannry, Joseph. (2010). Increasing the Safety of Healthcare Information Systems through Improved Procurement: Toward a Framework for Selection of Safe Healthcare Systems. Healthcare quarterly (Toronto, Ont.). 13 Spec No. 53-8. 10.12927/hcq.2010.21967.

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.

Lastdrager, E. (2011). *Securing Patient Information in Medical Databases* (Master's thesis, University of Twente).

Lee, T. F., Chang, I. P., Lin, T. H., & Wang, C. C. (2013). A secure and efficient password-based user authentication scheme using smart cards for the integrated epr information system. *Journal of medical systems*, *37*(3), 9941.

Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health information security in hospitals: The application of security safeguards. *Acta informatica medica, 24*(1), 47.

Ministry of Health (2010). Health Information System Policy document 2010-20130.

Muinga, N., Magare, S., Monda, J., Kamau, O., Houston, S., Fraser, H., ... & Paton, C. (2018). Implementing an Open Source Electronic Health Record System in Kenyan Health Care Facilities: Case Study. *JMIR medical informatics*, *6*(2), e22.

Mweebo, K. (2014). Security of electronic health records in a resource limited setting: The case of smart-care electronic health record in Zambia.

Neame, R. (2013). Effective sharing of health records, maintaining privacy: a practical schema. *Online journal of public health informatics*, *5*(2), 217.

Oluwasegun, S. C., & Odabi, O. I. (2011). Data security in health information systems by applying software techniques. *Journal of Emerging Trends in Engineering and Applied Sciences*, *2*(5), 775-781.

Peikari, H. R., T, R., Shah, M. H., & Lo, M. C. (2018). Patients' perception of the information security management in health centers: the role of organizational and human factors. BMC medical informatics and decision making, 18(1), 102.

Prislan, K., Mihelič, A., & Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PloS one*, *15*(9), e0238739.

Ravizza, A., De Maria, C., Di Pietro, L., Sternini, F., Audenino, A. L., & Bignardi, C. (2019). Comprehensive Review on Current and Future Regulatory Requirements on Wearable Sensors in Preclinical and Clinical Testing. *Frontiers in bioengineering and biotechnology*, *7*, 313.

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.

Samadbeik, M., Gorzin, Z., Khoshkam, M., & Roudbari, M. (2015). Managing the security of nursing data in the electronic health record. *Acta Informatica Medica*, *23*(1), 39.

Seymour, Dr. Tom & Frantsvog, Dean & Graeber, Tod. (2014). Electronic Health Records (EHR). 10.19030/ajhs.v3i3.7139.

Sharifian, R., Nematollahi, M., Monem, H., & Ebrahimi, F. (2013). Investigating the HIPAA Security Safeguards in theHIS of Shiraz University of Medical Sciences hospitals. *Health Inf Mang, 10*(1).

Sheen, S., Anitha, R., & Natarajan, V. (2015). Android based malware detection using a multifeature collaborative decision fusion approach. *Neurocomputing, 151,* 905-912.

Sontowski, S., Gupta, M., Chukkapalli, S. S. L., Abdelsalam, M., Mittal, S., Joshi, A., & Sandhu, R. (2020). Cyber-attacks on smart farming infrastructure. UMBC Student Collection.

Sotto, L. J., Treacy, B. C., & McLellan, M. L. (2010). Privacy and Data Security Risks in Cloud Computing. *World Communications Regulation Report*, *5*(2), 38.

Tempini, N., & Leonelli, S. (2018). Concealment and discovery: The role of information security in biomedical data re-use. Social studies of science, 48(5), 663–690.

Wilkinson, C. (2013). CYBER RISKS: THE GROWING THREAT.

World Health Organization. (2010). *Monitoring the building blocks of health systems: a handbook of indicators and their measurement strategies*. World Health Organization.

World Health Organization. (2016). *Consolidated guidelines on the use of antiretroviral drugs for treating and preventing HIV infection: recommendations for a public health approach*. World Health Organization.

Zaidan, B. B., Zaidan, A. A., & Mat Kiah, M. L. (2011). Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns. *Int. J. Pharmacol*, *7*(3), 382-387.

Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk management and healthcare policy*, *9*, 75.

Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. In *2010 IEEE 3rd International Conference on cloud Computing* (pp. 268-275). IEEE

Appendix 1: Research Questionnaire for MTRH a Health Records Staff.

SECURITY CONTROL MODEL FOR EHR FOR MOI TEACHING AND REFERRAL HOSPITAL

This questionnaire is purely for research and the information you will give shall be treated with high level of confidentiality. Thank you for your time.

SECTION ONE: GENERAL INFORMATION

(Please tick (√) the appropriate answer.)

1. Your Gender? Male [ ] Female [ ]

2. What is your age ………………….

3. What is your highest level of education?

a) Certificate [ ]

b) Diploma [ ]

c) Degree [ ]

d) Post Graduate [ ]

e) Secondary [ ]

4. Which department do you work in?

OPD's	[ ]	Chandaria Cancer Centre	[ ]
Central Records	[ ]	Private wing	[ ]
Mother and baby	[ ]	General wards	[ ]
Shoe for Africa	[ ]	Diagnostics services	[ ]

5. For how long have you been working in this institution?

a) Less than 1 year [ ] b) 1 - 5 years [ ] c) 6 – 10 years [ ] d) More than 10 years [ ]

SECTION TWO: CURRENT CONTROLS FOR EHR

5 Technical Security Controls

6. In your views, please rate the extent to which you agree with the following statements. Please tick (√) the appropriate answer**.** Use the scale of: 1 = strongly disagree, 2 = disagree, 3 = uncertain, 4 = agree, 5 = strongly agree

Indicator	1	2	3	4	5
There is a good antivirus protection that is designed to monitor computer systems and identify computer viruses or malware in real time					
The antivirus is updated frequently to keep pace with new viruses.					
The hospital has ensured that all the computers have passwords for protection of data.					
MTRH ensures that sensitive information is protected and only authorized personnel have access					
The hospital ensures that passwords are changed in periodic basis					
The health providers have access to patient information when needed.					
The hospital ensures that the medical records are protected against distortion while transmitting through electronic media.					

6 Physical Security Controls

Indicator	1	2	3	4	5
The hospital has ensured that the rooms and cabinets with patients' information are under lock and key to avoid unauthorized entry					
The motion detection systems are in place to detect any motion from potential intruders and raise the alarm					
The hospital has a closed-circuit Television (CCTV)system in place to record and detect any occurrence					
MTRH ensures that terminated or transferred employees access codes are terminated in a timely manner					
The hospital has door alarms to detect any unauthorized persons accessing the building					
The hospital ensures that individuals wishing to access the records departments obtain identifications before entry					

7 Administrative Security Controls.

Indicator	1	2	3	4	5
The hospital ensures accuracy of medical records by protecting the					

information against losses					
The hospital has ensured that issues of information security issues are addressed promptly					
Health records are handled by qualified personnel only?					
The hospital ensures healthcare providers only discuss a patient in need					
The hospital ensures that information security training takes place frequently.					
The hospital ensures that the user is only provided with necessary information					
The hospital has ensured that all the employees have knowledge of information security policies and guidelines					
The hospital ensures that employees handling patients records have IT knowledge to key in accurate data into the system					

SECTION THREE: EHR SECURITY CONTROL REQUIREMENTS

8 Technical Security Controls

7. In your views, please rate the extent to which you agree with the following statements. Please tick (√) the appropriate answer.

Use the scale of: 1 = strongly disagree, 2 = disagree, 3 = uncertain, 4 = agree, 5 = strongly agree

Indicator	**1**	**2**	**3**	**4**	**5**
The hospital ensures that Health records are backed up regularly to prevent loss of data.					
The hospital ensures that User rights are reviewed frequently					
The Smoke sensors and heat sensors are in place					
Intrusion Detection System software application and devices are in place to monitor computer systems for malicious activity and violation.					
There are system and network monitoring tools used to record log-ins and access to particular application to prevent unauthorized					

users.					
There is firewall that blocks any unauthorized activity within the system					
The hospital wireless network is encrypted so that unauthorized person doesn't understand the information					
The network being used by staff handling patient health records is isolated from the network being used by other members of staff not handling patient's health records					

9 Physical Security Controls

22. In your views, please rate the extent to which you agree with the following statements. Please tick (√) the appropriate answer.

Use the scale of: 1 = strongly disagree, 2 = disagree, 3 = uncertain, 4 = agree, 5 = strongly agree

Indicator	**1**	**2**	**3**	**4**	**5**
Power generators installed in the hospital in case of electricity failure					
Fire extinguishers are installed in rooms with patient's information					
Fire sprinklers have been installed in the hospital to suppress in case of fire outbreak.					
Uninterruptable power supply (UPS) installed in the Health Records section for power backup?					
Rooms with patient's information are fireproof and secure					
There is a monitoring station within the hospital to monitor daily occurrence.					
Temperature controls and dedicated air conditioning are in place					

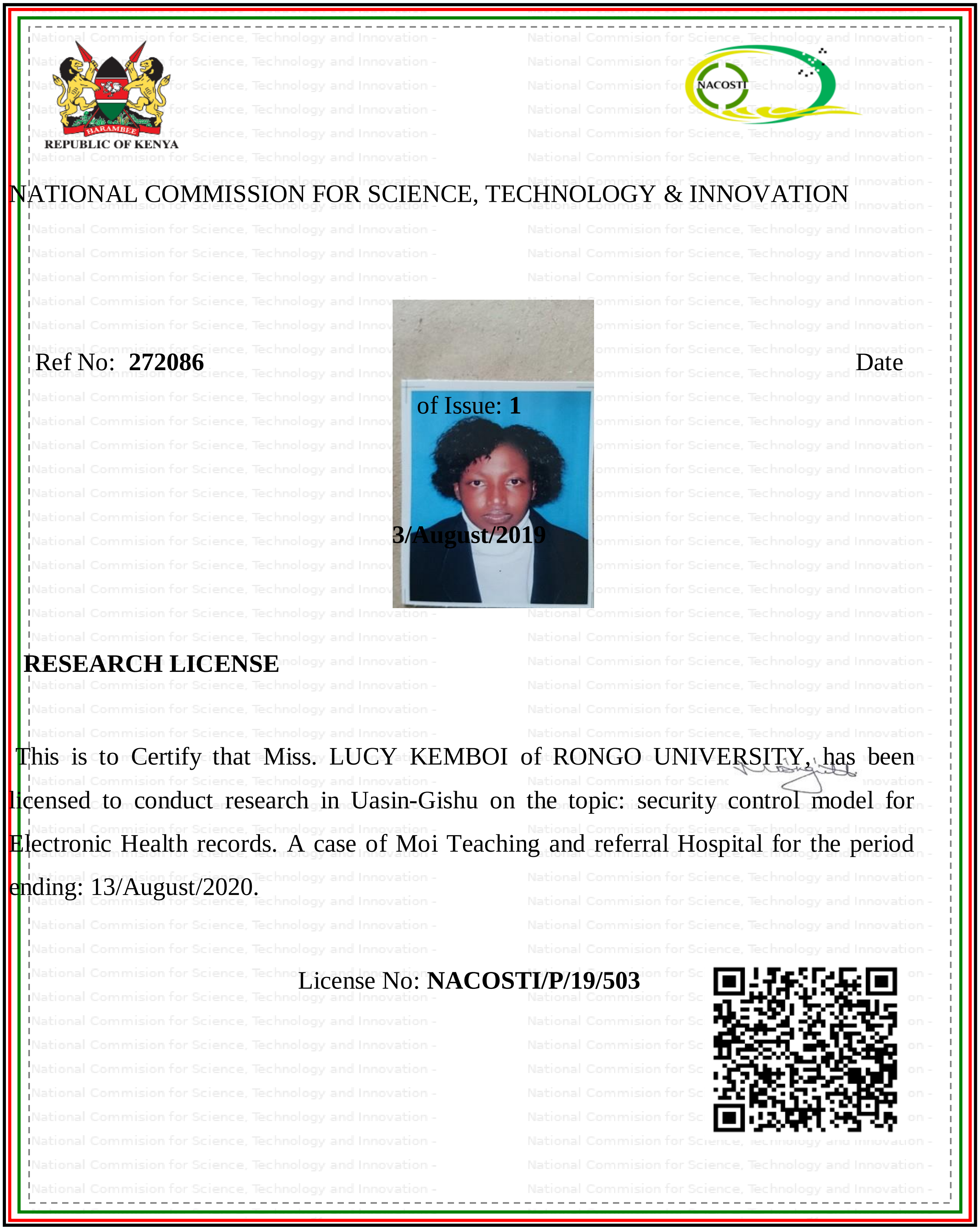
10 Administrative Security Control

23. In your views, please rate the extent to which you agree with the following statements. Please tick (√) the appropriate answer.

Use the scale of: 1 = strongly disagree, 2 = disagree, 3 = uncertain, 4 = agree, 5 = strongly agree

Indicator	**1**	**2**	**3**	**4**	**5**
Reports are reviewed regularly by the Chief Information security Officer					
There is a computer incident response team in place in case of the system failure					
The hospital has developed a plan of action and milestones for a continuous monitoring, identifying and addressing the system weaknesses in the security control implementation.					
The hospital management has developed and published a written access control policy on information security					
Information Security audit are done frequently to examine the security position of the hospital.					
There are procedures for removing access rights for a terminated employee, or unauthorized third party?					
The hospital has written procedures for the creation (registration) and deletion (deregistration) for user accounts.					
Users are required to sign access agreement.					
When a new account is created, the user is required to change to his/her password conforming to the hospital policy					
There are Procedures related to the security controls over access to the system					
Default passwords for systems, devices or applications are allowed anywhere in the hospital					

Appendix 2: Research Permit- NACOSTI



REPUBLIC OF KENYA

HARAMBEE

NACOSTI

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Ref No: **272086** Date

of Issue: **1**

3/August/2019

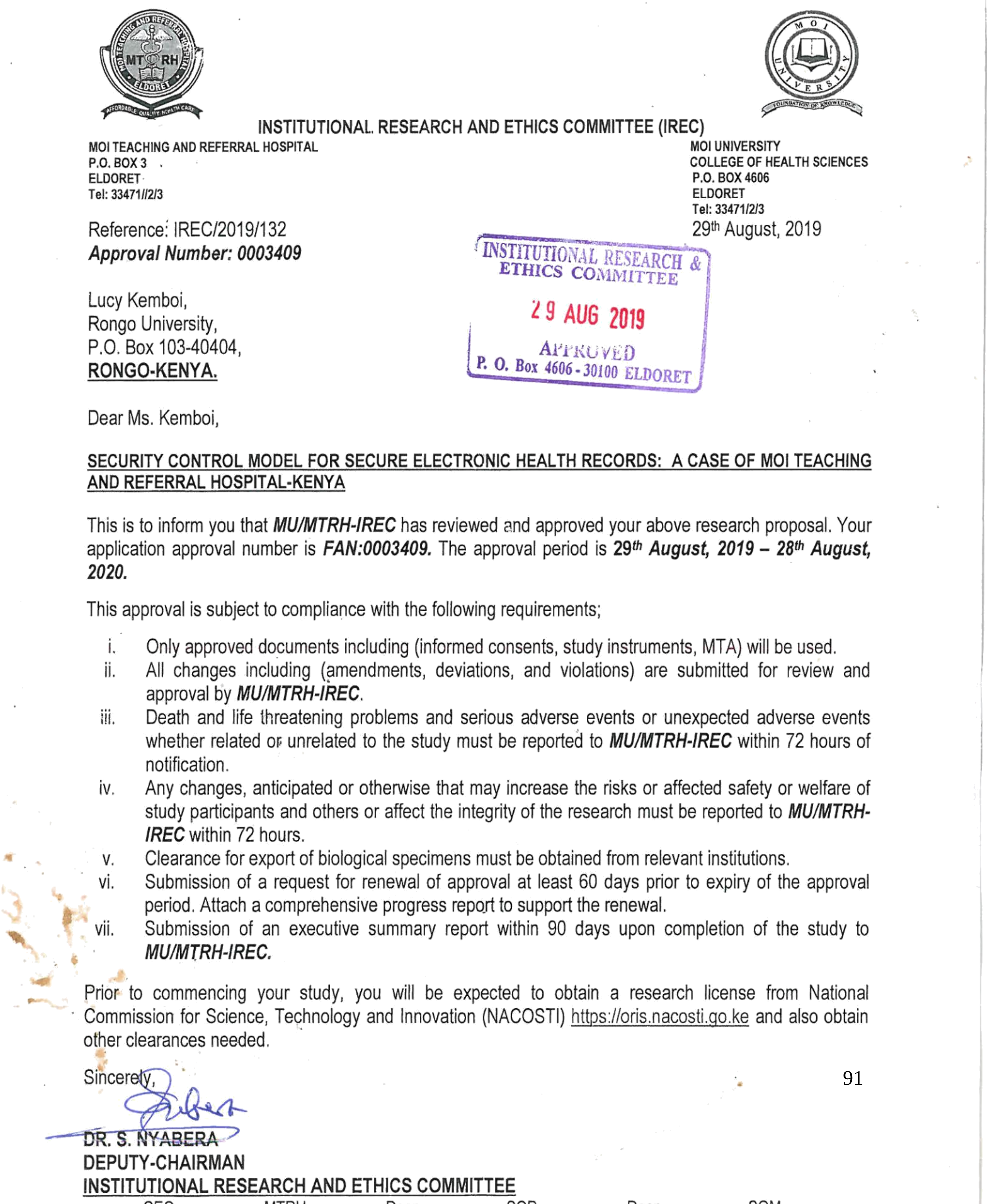
RESEARCH LICENSE

This is to Certify that Miss. LUCY KEMBOI of RONGO UNIVERSITY, has been licensed to conduct research in Uasin-Gishu on the topic: security control model for Electronic Health records. A case of Moi Teaching and referral Hospital for the period ending: 13/August/2020.

License No: **NACOSTI/P/19/503**

National Commision for Science, Technology and Innovation -

Appendix 3: Research Permit- IREC



INSTITUTIONAL RESEARCH AND ETHICS COMMITTEE (IREC)

MOI TEACHING AND REFERRAL HOSPITAL
P.O. BOX 3
ELDORET
Tel: 33471//2/3

MOI UNIVERSITY
COLLEGE OF HEALTH SCIENCES
P.O. BOX 4606
ELDORET
Tel: 33471/2/3

Reference: IREC/2019/132
Approval Number: 0003409

29th August, 2019

INSTITUTIONAL RESEARCH & ETHICS COMMITTEE
29 AUG 2019
APPROVED
P. O. Box 4606 - 30100 ELDORET

Lucy Kemboi,
Rongo University,
P.O. Box 103-40404,
RONGO-KENYA.

Dear Ms. Kemboi,

SECURITY CONTROL MODEL FOR SECURE ELECTRONIC HEALTH RECORDS: A CASE OF MOI TEACHING AND REFERRAL HOSPITAL-KENYA

This is to inform you that ***MU/MTRH-IREC*** has reviewed and approved your above research proposal. Your application approval number is ***FAN:0003409.*** The approval period is **29th *August, 2019 – 28th August, 2020.***

This approval is subject to compliance with the following requirements;

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by ***MU/MTRH-IREC***.
iii. Death and life threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to ***MU/MTRH-IREC*** within 72 hours of notification.
iv. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to ***MU/MTRH-IREC*** within 72 hours.
v. Clearance for export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days upon completion of the study to ***MU/MTRH-IREC.***

Prior to commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology and Innovation (NACOSTI) https://oris.nacosti.go.ke and also obtain other clearances needed.

Sincerely,

DR. S. NYABERA
DEPUTY-CHAIRMAN
INSTITUTIONAL RESEARCH AND ETHICS COMMITTEE

CEO MTRH Dean SOP Dean SOM