

**AN ENHANCED FRAMEWORK FOR ASSESSING HEALTH  
INFORMATION SYSTEMS SECURITY RISKS**

**HENRY M. ODIANGO**

**A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT FOR  
THE REQUIREMENTS OF THE AWARD OF DEGREE OF MASTER OF  
SCIENCE IN HEALTH INFORMATICS OF JARAMOGI OGINGA ODINGA  
UNIVERSITY SCIENCE AND TECHNOLOGY**

**© 2023**

## DECLARATION

This research project report is my original work and has not been presented in any other University for the award of degree.

Signature.....

Date..... 3<sup>rd</sup> AUGUST 2023


**HENRY M. ODIANGO**

**I153/4224/2017**

### Approval

This research thesis has been submitted for examination with my approval as the University Supervisors.

**PROF. SILVANCE ABEKA**

Signed.......... Date..... 5/8/2023

SCHOOL OF COMPUTING AND INFORMATICS

JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

**PROF. SAMUEL LIYALA**

Signed.......... Date..... 21/8/23

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

## **DEDICATION**

I dedicate this project to my family members for their prayers, time and encouragement which translated to the success of this project in my life. May God's blessings be with you abundantly.

## **ACKNOWLEDGEMENT**

Thanks be to Almighty God for enabling me to complete this Project. I greatly appreciate the technical guidance from my two Supervisors Professor Silvance Abeka and Professor Samuel Liyala for their guidance and great support throughout the project process. I also appreciate my Lecturer's for their unlimited support during the learning process. I cannot forget my classmates and fellow friend's for giving me the moral support.

My sincere gratitude goes to my Family members for their time and encouragement throughout the process. I also appreciate the School of informatics and innovative systems and the entire Jaramogi Oginga Odinga University of Science and Technology staff for the support during my learning period. I appreciate all the respondents from the six sub county hospitals in Siaya County, for creating time to complete the questionnaires making the completion of this research a big success. Last but not least special appreciation to my Boss at my place of work and the entire workmates for their support during the Research period

## ABSTRACT

The increasing digitization of health information enhanced accessibility, efficiency and quality of healthcare services. However, it has escalated cyber security threat, data breaches, unauthorized access to confidential information, manipulation, destruction, distributed denial of service, among others in addition, organizations are searching for an appropriate security framework for assessing information security risks. Although numerous frameworks are available, selection of the right framework is a challenge due to lack of prescriptiveness, standard, inconsistencies, complexity, compliance, cost, and certifications. All these negatively affect the information confidentiality, integrity and availability. The objective was realized by examining Health Information Systems Security Risks and strengths and weaknesses of existing frameworks. An enhanced Framework for assessing Health Information Systems Security Risks was developed. A descriptive cross – sectional design was adopted and questionnaire given to 61 respondents in the six Public Hospitals. Data was analyzed quantitatively using the Statistical Package for Social Sciences (SPSS version 20) and Results presented in tables, charts and graphs. Results indicated that confidentiality of information was good (use of passwords 96.8%, policies 91.9%, and access privileges 68.8%). Integrity of information was poor with written information security manager's responsibility 39.5%, monitoring of electronic systems 40%, creation of audit logs 54%, reviewing audit logs 51.5%. Availability of information was good (availability of computer inventory 69.9%), regular updates of inventory 61.3%, updates of patient data on laptops 68.2%, sharing of data confidentiality and security policy 36%, and backups of audit logs 51%. On assessment of existing security frameworks, HIPAA lacks complete valid risk analysis, not certifiable, safeguarding electronic protected health information only, does not regulate emails ,not using encryption, and commitment on security is verbal.ii/IEC 27001 framework is expensive, requires specific IT budget, special expertise, and more time to apply in public hospitals. NIPP framework is expensive, and uses consequence's assessment which is outside the scope of this study. The study concludes that the three frameworks assessed did not meet desired standards leading to development of an enhanced Framework. The study recommends training of persons authorized to access patient's information, avail defined roles of information security manager, and review data accuracy

## TABLE OF CONTENTS

DECLARATION .....	<a href="#">ii</a>
DEDICATION .....	iii
ACKNOWLEDGEMENT .....	iv
ABSTRACT.....	v
TABLE OF CONTENTS.....	vi
LIST OF TABLES .....	x
LIST OF FIGURE.....	xi
CHAPTER ONE: INTRODUCTION.....	1
1.1 Background of the Study .....	1
1.2. Problem Statement	
1.3 Objectives of the Study.....	5
1.3.1 General Objective .....	5
1.3.2 Specific Objectives .....	5
1.4 Research Questions.....	5
1.5 Significance of the Study.....	5
1.6 Scope of the study.....	6
1.7 Assumptions of the study .....	6
1.8 Limitations of the Study .....	6
1.9 Definition of Terms and Concepts.....	6
1.10 Abbreviations and Acronyms.....	7
CHAPTER TWO: LITERATURE REVIEW	10
2.1 Introduction .....	10
2.2 Theoretical Review.....	10
2.2.1 Control and Auditing Theory .....	10

2.4 Risk Management Theory .....	11
2.5 Threats and Vulnerabilities.....	12
2.6 Information Security and Framework.....	13
2.7 Frameworks for assessing information Systems Security Risks .....	17
2.7.1 Health Insurance Portability and Accountability Act.....	17
2.7.2 ISO/IEC 27001 Framework.....	20
2.7.3 Hitrust Framework.....	21
2.7.4 national infrastructure protection plan- risk management framework .....	24
2.8 Conceptual Framework.....	25
Conceptual Framework.....	27
2.8 Summary of Gaps .....	28
<b>CHAPTER THREE: RESEARCH METHODOLOGY .....</b>	<b>29</b>
3.1 Introduction .....	29
3.2 Location of the Study .....	29
3.3 Research Design .....	29
3.4 The Target Population .....	29
3.5 Sample Design.....	30
3.6 Data Collection Instruments .....	31
3.7 Piloting of the Research Instrument .....	31
3.8 Validity and Reliability .....	31
3.9 Data Collection Procedures. ....	32
3.10 Data Management and Analysis .....	32
3.11 Ethical Considerations .....	32
3.12 Summary of Research methodology.....	32
<b>CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSIONS 34</b>	
4.1 Introductions.....	34
4.2 Demographic Characteristics of the Respondents .....	34

4.2.2 Distribution of Respondents by Age .....	34
4.2.3 Distribution of Respondents by Professional Background.....	35
4.2.4 Distribution of Respondents by Level of Education .....	36
4.2.5 Distribution of Respondents by the Department in which they work .....	36
4.3 Objective one: Assessment of Health Information Systems Security Risks .....	37
4.3.1 Information Confidentiality .....	38
4.3.2 Data Integrity .....	40
4.3.3. Information Availability .....	44
4.4. Objective two: Assessed existing frameworks for assessing Health Information Systems Security Risks.....	45
4.5 Objective three: Develop Enhanced Framework for Assessing HIS Security and Risk .....	48
4.6 Discussion of Findings .....	52
4.6.1 Objective one: To examine existing Health Information Systems security risks.....	52
4.6.1.1 Information confidentiality .....	52
4.6.2 Data integrity .....	53
4.6.3 Information Availability .....	54
4.6.4 Discussion on existing frameworks .....	55
Objective 2: Assessment of Existing Frameworks for assessing HIS Information Security Risks .....	55
4.6.5 Summary of the assessment of the three Information Security Frameworks.....	58
4.6.5: Developed Enhanced Framework for assessing HIS Security Risks .....	63
4.6.6. SUMMARY OF DATA ANALYSIS, RESULTS AND DISCUSSIONS.....	65
<b>CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS</b>	<b>66</b>
5.2 Summary of the Findings .....	66
5.2.1 Objective one: Assessing Health Information Systems Security Risks .....	66



5.2.2 Objective two; Assessing existing Frameworks for assessing HIS Security Risks .....	69
5.2.3 Developed Enhanced Framework for assessing HIS security Risks .....	70
5.3 Conclusion .....	71
5.4 Recommendations .....	73
5.5 Suggestions for Further Studies.....	74
6.6 Disclosure of conflict of interest .....	74
REFERENCES .....	75
ANNEXES	
Annex I: Letter of Transmittal.....	87
Annex 2: Informed Consent .....	88
Annex 3: Questionnaire .....	89
ANNEX 4: WORK PLAN .....	98
ANNEX 5: RESEARCH BUDGET .....	99
ANNEX 6: JOOUST ETHICAL RESEARCH POLICY (ERC) APPROVAL .....	100
ANNEX 7: NACOSTI APPROVAL.....	101
ANNEX 8: COUNTY DIRECTOR OF HEALTH APPROVAL .....	102

## LIST OF TABLES

Table 1	Published Table for Sample size	28
Table 2	Proportionate Stratified Sampling	29
Table 3	Distribution of Respondents by Gender	34
Table 4	Distribution of Respondents by Age	34
Table 5	Distribution of Respondents by Professional Background	35
Table 6	Distribution of Respondents by the Level of Education	36
Table 7	Distribution of respondents by the department where they work	37
Table 8	Information confidentiality	39
Table 9	Data Integrity	41
Table 10	Information Availability	45
Table 11	Strengths and weaknesses of the existing Frameworks	47
Table 12	Characteristics, strengths and weaknesses of reviewed Frameworks	62

## **LIST OF FIGURE**

Figure 1	HIPPA Framework	16
Figure 2	SO 27001	19
Figure 3	NIPP Framework	22
Figure 4	Conceptual Framework	26
Figure 5	Use computers to perform duties	39
Figure 6	What employees use Computer for	40
Figure 7	Proposed enhanced Framework	52
Figure 8	Proposed Enhanced Framework	69



## **CHAPTER ONE: INTRODUCTION**

### **1.1 Background of the Study**

In a typical scenario, patients may seek treatment from numerous hospitals during their lifetime. Consequently, they leave scattered healthcare records in different hospitals. The implications are that accessing previous healthcare records belonging to these patients presents some uphill challenges. According to Chelladurai (2022) these fragmented records result in poor management of patient data. It is also possible for each of these hospitals to have its own healthcare record management software. Therefore, there is lack of networking among the health service providers which imply scattered healthcare records in diverse disconnected places Mead CN. (2006). As explained by Houlding D (2011), devoid of integrated data management coupled with isolated healthcare record from medical labs, insurance firms and pharmaceutical manufacturers result in the breakdown of health information across providers. However, the rapid development of information technology has facilitated the development of Telecare Medicine Information System (TMIS) as well as Health Information Systems (HISs). (Xiao et al.,2021). These systems according to (Nyangaresi VO et al,2021) comprise of medical sensors, smart robotics and smart phones that help patients in remote locations to access health care services. Using TMIS, it has become possible for doctors to utilize robots and smart digital sensor to carry out surgeries. (Javed ,2020 & Sarwar,2019). In addition, (Zeng X. et al,2016) explain that technology integration in the healthcare industry has seen the conversion of paper-based health records to electronic records. The goals of this conversion may include enhanced productivity and efficiency in healthcare facilities. It also makes it possible for the electronic personal health information (ePHI) to be easily accessible, permitting global health networking.

In the past, information systems challenges are increasing, and, there is need since the topic of information security is dominating challenges worldwide as a concern to many organizations. In this study, more focus is given to the assessment of information security risks as a major concern of strategies employed to control information insecurity

A Health Information System (H.I.S.) is defined as a system that deals with the collection, procession and storage of all data and information created and handled in a

hospital. (Winter, 2001). The term Health Information System is used interchangeably with Hospital Information System. (HIS) and at times as Health Management Information System (HMIS), and even at times Healthcare Information Systems (HCISs) which have been defined as powerful ICT-based tools able to make health care delivery more effective and efficient (P Locatelli et al., 2012).

The investment of Information Technology (IT) in Hospitals began during the 1960s. 'IT' was first used to support billing and financial services. The History of Medical Informatics in the United States (Collen, et al., 2015). Subsequently, the IT applications started to support and monitor basic clinical activities such as Laboratory and Pharmacy process management as well as documentation of patients' radiology histories. Measuring information technology capability, (Zhang et al., 2008).

The continued adoption of HISs has led to the enhancement of accessibility, efficiency and quality of healthcare services. It has also resulted in reduced medical errors, better healthcare, increased efficiency and accuracy of patient care and administration. Ngafeeson MN. (2015). According to Siyal et al (2019) Secure and scalable data sharing is critical for healthcare decision-making system. However, the traditional fragmented healthcare record systems impede effective information flow and hence prevent patients from making sensible treatment decisions. On the other hand, TMIS enables the patient from any remote location to contact the hospital medical server to share and access required information over some public channels. (Nyangaresi VO et al ,2022). As explained in Kumar V (2019) TMIS has made it possible for patients to access doctor's telemedicine services over the internet. In so doing, TMIS accelerates the convenience of healthcare services access to patients at their place of preference providing real-time remote diagnosis (Shamshad et al ,2022). As discussed by (Shamshad et al,2022) these digital healthcare technologies have revolutionized the healthcare sector, enabling efficient collection, storage and access to ePHI.

Although TMIS, HIS and ePHI have numerous advantages, they are faced by many challenges. For instance, large volumes of private and sensitive patient data are stored in TMIS which can result in grave consequences if maliciously accessed or leaked (Amin R. 2018). This calls for safe storage, transmission as well as the reservation of integrity in these TMIS. Kui X. (2021) and Nyangaresi VO (2022). As discussed by

(Xiao & Liang 2021) TMIS has various setbacks such as false authentication, key losses, and failure of the data node that brings forth serious loss of data. Therefore, security is key for the safe transmission and storage of electronic patient records. Song J, (2020), Al Sibahee MA. (2022), Wang W. (2021), Javed AR. (2020), and Zhang L. (2021).

The identity authentication process of TMIS occurs in a public channel, which is vulnerable to attackers. Attackers can disrupt the authentication process through eavesdropping, interception, and forgery method, and launch malicious attacks such as forgery attacks, replay attacks, and side-channel attacks Nyangaresi VO. (2021). These attacks can lead to malicious access, data loss and intellectual property infringement. Liang W. (2020). During the development and implementation of TMIS and HIS, security should be incorporated in early stages. (Justinia 2019 & Dharminder 2021). In addition, interoperability between healthcare systems should be assured so that there is efficient exchange of health records between providers Abouelmehdi.(2018) .Though internet-facilitate diagnosis and treatment, many threats can be launched to the exchanged messages over the open internet .Nyangaresi VO. (2021) .In addition, the design of new systems to address security challenges in digital healthcare record systems must uphold interoperability, secure transfer, storage, and efficient retrieval .Burghard C. (2012).This will help healthcare breaches vectors such as Worms, Trojan horse, computer viruses, hacking and ransomware .Hummelholm A.(2022).However, ensuring the security of massive personal health information (PHI) being collected by numerous electronic devices has been noted to be cumbersome .Beck EJ.(2016) .As such, the assurance of perfect confidentiality, integrity, secrecy and security in TMIS remains challenging .Shamshad ,S.(2022)

To prevent resource abuse and malicious attacks, authentication is normally the first step. Nyangaresi VO. (2022) Here, the TMIS need to validate the identities of all network entities before access is granted. Additional security measure such as antivirus, encryption, firewalls, audit logs, usernames and passwords can also be implemented. Moreover, legislative and regulatory frameworks can be implemented in healthcare facilities to enhance security. For instance, based on the Health Insurance Portability and Protection Act (HIPAA), healthcare providers need to put in place standards and policies to govern the security and protection of electronic health

and medical information. Failure to comply with personal data protection legislation, healthcare facilities may face civil and legal penalties Chuma KG. (2022). In the long run, such non-compliance may cause some harm to the employees or patients Asija R. (2014). The Data Protection (General) Regulations, 2021. Prinsloo, P., & Kaliisa, R. (2022).

## **1.2. Problem Statement**

Threats from cybercrime is on the upward trend in developing countries in Africa more than other countries worldwide leading to a call for more attention. The main causes of cybercrime are attributed to vulnerable systems, poor cybercrime legislations, lack of proper cyber security guideline, policies practices, and under-skilled professionals, as a result Africa has become a continent of heightened cybercriminals, Kshetri (2019). Many researchers have appreciated the applicability of existing frameworks to auditing cyber security (ISACA & Protiviti, 2020; Jreissat et al., 2018; Otero, 2019; Yeboah, 2013). However, despite many efforts towards cybersecurity standardizations and cyber governance standardization, there is still no consensus on a standard framework (Savaş and Karataş, 2022).



### **1.3 Objectives of the Study**

#### **1.3.1 General Objective**

The general objective was to develop an enhanced framework for assessing Health Information Systems Security risks

#### **1.3.2 Specific Objectives**

The study was guided by the following specific objectives:

1. To examine existing Health Information Systems security risks
2. To assess existing frameworks for assessing HIS security risks
3. To develop an enhanced framework for assessing HIS security risks
4. To validate the developed enhanced Framework for assessing HIS security risks

### **1.4 Research Questions**

1. Which are the existing HIS security risk?
2. Which are the existing frameworks for assessing HIS security risks?
3. Which is the developed framework for assessing HIS security risks?
4. which is the validated developed enhanced framework for assessing HIS security risks?

### **1.5 Significance of the Study**

This study developed a framework for assessing HIS security risk to ensure confidentiality, integrity, availability and accountability of patient's information during and after treatment. The study adds value to policy makers as it addresses security of Clinical IT systems as opposed to only looking at administration and financial transactions systems. The study is an asset to future research scholars as it reviewed existing frameworks for assessing HIS security risk in the interconnected world full of cyber insecurity. Nearly all organization's need information to operate and disruption to information lead to a security breach of an organization's operations and therefore, filling this gap makes essential contribution to the body of knowledge.

## **1.6 Scope of the study**

This study was conducted in Siaya County and focused on assessing existing HIS security and risk, examined existing frameworks for assessing HIS security developed a framework for assessing HIS security risk. The study used descriptive cross-sectional design and data was collected by the two research assistants. Ethical approval was obtained from the Post graduate Ethical and Review Committee of Jaramogi Oginga Odinga University of science and Technology and the County Director of Health and Sanitation, Siaya County. Licence to conduct the research was given by the National Commission for Science, Technology & Innovation (NACOSTI). The study population was staff working at the six public hospitals, both male and Female, the findings was shared with all the stakeholders through written report.

## **1.7 Assumptions of the study**

Respondents provided the Information required within the time stipulated for data collection. The researcher assumed resources to undertake research would be available and that there would be no major constraints to the assessment and that the respondents would be honest, truthful and transparent, in their responses to the assessment questions. There would be no outbreak of diseases leading to restrictions of movements within the County

## **1.8 Limitations of the Study**

The study was done only in six Sub County Hospitals in Siaya County, these Hospitals are owned by the ministry of Health and managed by the County Government

## **1.9 Definition of Terms and Concepts**

**Health Information Systems:** A system that collects, stores, **processes**, analyses, and transmits data **in** various levels

**Risk Assessment**, the process of identifying risks, conducting risk analysis to determine the likelihood and impact of the risks, quantifying the risks

**Security Framework:** Standards and guidelines used for assessing information security risks in organizations

**Electronic protected Health Information:** The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information

**NIPP: National** information protection plan is a framework for assessing security of the information system in various organizations

**Public Hospitals: Public** Hospital is a Hospital owned and operated by the Government

## 1.10 Abbreviations and Acronyms

AICP	American Institute of Certified Public Accountants
CIA.	Confidentiality Integrity and Availability
COBIT	Control Objectives for Information and Related Technologies
CoT	Cycle of trust
CSF	Common security framework (CSF)
CDSS	Computer Decision Support System
CEO	Chief Executive Officer
CI/KR	Critical infrastructure and Key Resources
DHS	District Health Systems
DHS	Department of Homeland security
EPHI	Electronic Patient Health Information System
EHR	Electronic Health Records
GOK	Government of Kenya
HIS	Health Information System
HHS	Health and Human Services
IT	Information Technology
ISAC	Information Systems Audit and Control Association
ISMS	Information Security Management system
MOH	Ministry of Health
OECD	The Organization for Economic Co-operation and development
PHR	Personal Health Records
SQL	Structural Quarry Language
SIS	Swedish information system
WHO	World Health Organization
ICT	Information Communication Technology
HMIS	Health Management Information Systems
SD	Standard Deviation
IQR	Interquartile Range
NIPP	National Information Protection Plan
SCH	Sub County Hospital
EPHI	Electronic Patient Health Information System
DHIS	District Health Information Systems

NIST	National Institute of Standards and Technology
MFL	Master Facility Listing
ISO	International Organization for Standardization
ISF	An Importer Security Filing
BT	Block Chain Technology
PHI	Personal Patient Information
TMIS	Tele Medicine Information System
IDS	Intrusion Detection System
HITRUST	Health Information Trust Alliance
NACOSTI	National Commission for Science, Technology & Innovation
HIPAA	Health Insurance Portability and Accountability Act
PH	Public Health

## **CHAPTER TWO: LITERATURE REVIEW**

### **2.1 Introduction**

This chapter reviewed literature related to a framework for assessing Health Information security risks. The literature review was guided by the study objectives and began by focusing on examining existing HIS security risks, next to assess available frameworks for HIS security risks, and developed an enhanced framework for assessing security of HIS risks. The study was anchored on two theories which are Control and audit theory and risk management theory. These formed the basis for this study

### **2.2 Theoretical Review**

This study was grounded on two theories which are control and audit theory and Risk Management theory

#### **2.2.1 Control and Auditing Theory**

Control and auditing Theory postulates that, organizations need to establish information security control measures which upon implementation, should be followed by conducting auditing procedures to evaluate the performance of control in place. Information security management is considered by many researchers as forming part of control systems. According to the Information Systems Audit and Control Association (2015), the term ‘audit’ refers to the formal assessment and inspection to check the compliance to standards and guidelines, to validate a standard or set of guidelines, and to find out if records are precise, and targets are being met. From an alternative perspective of information security control, components include; organizational security, security policy, personnel security, communication and operation security, system development and maintenance, assets classification and control, physical and environmental security, business continuity planning, and compliance. ISO/IEC 17799. (2000).

Another theory that relates to information security standards is the COBIT, which is an IT management framework developed by the ISACA to help businesses develop, organize and implement strategies around information management and governance. COBIT is an IT management model that emphasizes two major internal control

models that is; holistic operation control model and focus on information technology model. COBIT is a guideline which is of high level for IT resources and entails application techniques, data, personnel and hardware. COBIT achieves the organizations objectives by balancing the risk, as well as directing and controlling measures.

According to COBIT, there is need for organizations to refer to information security standards and establish information security strategies leading to formation of IT security control systems. COBIT recommends that once organizations have implemented these controls systems, then information audit should be done regularly to assess the performance of the controls in place.

In summary, control and audit Theory is good as it spells out that in regards to control systems, information security is achieved through these functions;

Information security= f (establishment of control systems, implementation of control systems, information audit)

Establishment of control systems = f (security strategies, security standards)

### **2.2.2 Risk Management Theory**

Based on Risk Management Theory, the threats and vulnerabilities regarding information security could be estimated and assessed by doing risk analysis and evaluation. The outcome can aid in planning information security requirements and risk control measures. The aim is to reduce the information security risk to an acceptable level within the organization. Risk management is a key process that entails an ongoing identification, assessment, and mitigation of risks to sustain an acceptable level. It is a comprehensive term that includes risk assessment as one of its elements. Silva et.... al. (2018). By applying information Security Risk management, an organization can protect information in a cost-effective way. In a separate study defines Risk management as the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level, the study further states that an effective risk management process is an important component of a successful IT security program, and that the purpose of an organization's risk management process is to safeguard the organization and its ability to perform their mission, not just its IT

assets. Stone burner *et...al.* (2002). The risk management process should not only be seen as a technical function carried out by the IT experts who operate and manage the IT system, but majorly as a fundamental management function of the organization.

The combination of risk assessment and risk control enable information security risk to be reduced to an acceptable level. The relationship between the risk analysis and risk control can therefore be summarized in four simple ways as illustrated below;

Risk management theory is good in that, it states the relationship between risk assessment and risk control which leads an organization into lowering the risk to an acceptable level; however, it does not include information security policy, capacity building of staff, behavior Change among staff and commitment of top leadership which are required to ensure long lasting solutions to information security in an organization.

### **2.3 Threats and Vulnerabilities**

Many threats, attacks, risks and vulnerabilities lurk in Telecare Medicine Information System (TMIS,) HIS and ePHI systems. For instance, Conaty-Buck S (2017) has identified distributed denial of service (DDOS), privilege escalation, phishing, spoofing and password guessing attacks as being frequent and consequential in healthcare organizations. In addition, malware, worms, spyware, viruses, Trojans, ransomware, rootkits, adware and sniffers have been found to be serious issues in the healthcare sector. Moreover, hazards such as tornado, floods and fires may destroy health information and systems (Pankomera 2017). As explained by Bernard R, (2020) attacks and threats against hospitals, medical devices and healthcare entities are on the rise. Here, the threat agent utilizes techniques such as phishing, botnets, man-in-the-middle and SQL injections to exploit various vulnerabilities in hospital systems, networks. Nyangaresi VO. (2021). These vulnerabilities may be in software applications, system security procedures, regulatory compliance, policies and procedures. Chuma KG. (2022). The motivation behind these attacks range from financial gains to political gains.



## 2.4 Information Security and Framework

To curb these attacks and threats, security frameworks have come up with security control mechanisms that all healthcare facilities need to adopt in order to thwart, detect or minimize vulnerabilities, attacks and threats against their electronic healthcare systems. The three pillars for securing HIS systems comprise of administrative, physical and technical security controls. (Kruse & Ives 2017). The administrative controls may include, staff training, disciplinary actions for violation of policies, rules and procedures for assigning access to HIS, security policies, inventory management, maintenance of audit trails, methods for incident reporting, Risk assessment and data review as well as accountability. Andriole. (2014) On the other hand, physical security controls encompass proper device disposal, device isolation and emergency contingency protocols. Ngethe, N. S. (2021) states that components of physical security measures include Lock and key, secure server rooms, surveillance, and installation of fire alarms and burglary. Khajouei et al., (2017) found out that physical security controls (like lock-and key) reduced chances or exposure of confidential data to unauthorized personnel. In another study by Wanyonyi, E. et al, (2017) On their part, technical security controls include biometrics, access control systems. Nyangaresi VO. (2021). Passwords, encryption, antivirus, firewalls, radio frequency identification (RFID) and Intrusion Detection System (IDS). Lemke, J. (2013). According to Marutha (2019) Healthcare organizations and hospitals subscribe to healthcare legislation's that are regulated by the concerned jurisdiction. These regulations and legislation's offer the groundwork for enhanced and resilient healthcare systems. In this regard, various techniques have been put forward to protect HIS as well as the data exchanged in TMIS.

To provide interoperability and secure way to store and exchange information, block chain technology (BT) has been adopted. Panigrahi A. (2022). Here, BT helps in the maintenance of patient electronic health records (EHRs) and electronic medical records (EMRs) for numerous telemedicine, medical devices, and billing systems. The deployment of public block chain serves to minimize the requirement for dependable nodes during information exchanges. Abdellatif AA. (2022). As pointed out by Kavathekar SS. (2019). Privacy safeguards must be incorporated in any block chain architecture employed to build healthcare applications. In HIS, BT can be utilized to offer data consistency of the health record. Zhang P. (2017). This serves to

enhance quality, facilitate patient and physician coordination and hence improve the overall outcome. BT can also permit patient-centric control of healthcare data sharing among the healthcare facilities. Gordon WJ. (2018). Essentially, it acts as a clinical data repository that offers distributed ledger record of all medical events. By so doing, it permits healthcare providers to have seamless access to patient electronic health records. Chelladurai U. (2022). This helps address the traditional fragmented healthcare record keeping issues where access to this data presents some challenges especially when the patient is in critical condition. To enhance data management, several block chain based workflows for the healthcare environment have been designed in Khatoon A. (2020). Similarly, block chain medical record storage and sharing systems have been designed in. Azaria A (2016) and Zhou L. (2018). while patient-centric healthcare data management system has been developed in for storage and privacy enhancement. Al Omar A. (2018). On the other hand, block chain-based apps for healthcare have been presented in. Zhang P. (2018). However, block chain has high storage and computation complexities. Nyangaresi VO. (2021)

Another important technology for healthcare security enhancement is the physically unclonable function (PUF), which generates unique and unpredictable response data for any challenge information. Maurya PK. (2018) For instance, an access control and authentication scheme by. Xiao L (2021) combines PUF and Elliptic Curve Cryptography (ECC) to ensure the safety of TMIS. Similarly, the verification scheme by. Xu H, Ding J. (2018). incorporates PUF in its design. However, this scheme cannot withstand secret disclosure and de-synchronization attacks. Bendavid Y. (2018). In addition, a PUF based privacy protection access control scheme is developed in Gope P. (2018). while a lightweight access control protocol is introduced in. Liang W. (2018). However, PUF-based schemes have stability issues Nyangaresi VO. (2021). Moreover, the protocol by. Liang W. (2021) can potentially expose the identity information of the tag and hence is susceptible to traceability attacks. Apart from PUF, intrusion detection systems can also help secure HIS. For instance, a secure identity authentication and intrusion detection scheme is presented in Liang W. (2021). while an ECC based access control protocol is introduced in Farash MS. (2016). Similarly, lightweight and secure authentication protocols are developed in. Zhang, L (2016) and Siddiqui Z. (2014). However,

identity based schemes have key escrow issues. Nyangaresi VO. (2021). while the scheme in Farash MS. (2016). offers only a one-way verification function. On its part, the protocol in Zhang, L. (2016) is vulnerable to packet replays, identity and password guessing attacks.

An efficient, secure and robust protocol has been presented in Madhusudhan R. (2019) Unfortunately, this protocol is vulnerable to traceability, stolen smart card, privileged insider, packet replays, server impersonation, identity and password guessing attacks. Dharminder D. (2021). Sureshkumar V. (2020) On the other hand, an access control and key establishment protocol is presented in. Xu X, Zhu P. (2014). Although this scheme has low authentication costs, it cannot withstand replay attacks. Nyangaresi, VO. (2021). In addition, the password cannot be updated correctly. Based on chaotic maps, a novel authentication protocol is developed by Guo C, Chang. (2013). However, this protocol cannot offer both intractability and anonymity. an improved scheme is presented in Hao X As. (2013). such, Unfortunately, this enhanced protocol cannot withstand stolen smart card attacks. Jiang Q. (2014). To prevent man-in-the-middle and replay attacks, a three-factor access control protocol is developed in. Amin R. (2015). However, this scheme is still vulnerable to simulation and internal attacks. Wazid M. (2016). On the other hand, a radio frequency identification scheme has been developed in. Wang X. (2022). that is shown to be lightweight and secure. This scheme is shown to resist forgery, de-synchronization, replay and denial of service attacks. Unfortunately, for the scheme in. Wang X. (2022) the real identities are exchanged in plain text between the tag and its reader. Nyangaresi VO. (2022). On the other hand, a digital signature based technique is presented in. Amir Latif RM. (2020). In another study an RSA based authentication scheme for securing transaction history of the patient developed by. Dharminder D. (2020). However, this technique has lower efficiency due to the utilization of modulo exponentiation operations. Based on chaotic maps, secure remote access control methods are introduced in. Li CT. (2018). and. Dharminder D. (2020). However, chaotic map based protocols are susceptible to stolen smart-card, impersonation, identity and password guessing attacks. Dharminder D. (2021). In addition, the approach in. Li CT. (2018). cannot withstand side-channel attacks, while the technique in. Li CT. (2018).is vulnerable to offline password guessing and impersonation attacks. Nyangaresi VO. (2021). Similarly, a patient-centric data sharing system is developed by. Angelis J. (2019). Based on machine learning

algorithms for anomaly detection.

According to another study to offer string location confidentiality in healthcare system, an efficient access control scheme is presented in. Tewari A. (2020). However, this technique is vulnerable to replay and random nonce exposure attacks. An access control technique is introduced in. Li CT. (2015). To offer database and reader authentication so as to thwart sever loss attacks. However, this approach fails to offer anonymity as well as protection against both replay and asynchronous attacks. Zhou Z. (2019). On the other hand, secure and efficient protocol is introduced in. Jiang Q. (2018). To secure telemedicine services. Unfortunately, this scheme is inefficient due to massive message exchanges during session key derivation. To address these issues, a secure and efficient authentication protocol is developed in. Wu F. (2018). While another new design for telemedicine services protection is developed in. Radhakrishnan N. (2019). Unfortunately, these two protocols are vulnerable to stolen card information, identity and password guessing attacks. To secure private data in healthcare sector, a scheme based on secondary residue and timestamp is presented in Zhou Z. (2019). This technique is shown to withstand replay attacks. However, it fails to protect against asynchronous attacks and it also incurs high implementation costs. This is detrimental to cost constrained. Alsamhi SH. (2022). TMIS system components such as medical sensors. To address this, an efficient authentication method is developed in. Chander B. (2022). Although the scheme in. Zheng L. (2018). Offers mutual authentication, it is susceptible to replay attacks. Safkhani M. (2019). This problem is addressed by the El-Gamal cryptographic system developed in. Salem FM. (2020). On the flip side, this approach incurs high storage costs. Nyakomitta, P. S. (2021).

A telecare medicine information systems presented in. Islam SK. (2014). Has a number of vulnerabilities that were addressed by the scheme developed in. Jian G. (2016). However, the technique by. Jian G. (2016) is vulnerable to man-in-middle, offline password guessing, user and server impersonation attacks. To share medication history in a secure and efficient way, authors. Li P, Nelson SD. (2019). Have developed a public key based method. However, the usage of this public key infrastructure may lead to high overheads. Nyangaresi VO. (2022). On the other hand, an authentication protocol for remote healthcare systems is introduced in. Ravanbakhsh N. (2018). Unfortunately, this method is vulnerable to session-specific

temporary information attack. Ostad-Sharif A. (2019). Although the protocol developed by. Qiu S. (2017). is efficient and secure, it cannot provide anonymity and is susceptible to impersonation and password guessing attacks. Nyakomitta SP. (2014). Kumari S. (2021). This anonymity challenge is addressed by the PUF based scheme developed in. Shamshad S. (2021). Based on RFID, a privacy preservation protocol is presented in. Fan K. (2018). Securing remote medical data. However, this approach cannot withstand de-synchronization, denial of service and replay attacks. To solve these issues, an identity-based remote user authentication scheme is developed in. Barman S. (2019). Unfortunately, this approach is vulnerable to stolen verifier, impersonation and secret key leakage attacks. Ali Z, Hussain S. (2020). In addition, it has some key escrow issues. Nyangaresi V.O. (In the 6th International Conference, 605-612). Although the scheme in. Ostad-Sharif A. (2019). solves some of these challenges, it is shown to be susceptible to password guessing, impersonation and session key hijacking attacks. Nikooghadam M. (2020). To uphold security among the involved entities in the TMIS, two schemes are developed in. Limbasiya T. (2021)]. However, these protocols cannot withstand stolen verifier and cloning attacks. In light of the above HIS security challenges, this paper sought to develop an enhanced framework for assessing HIS security risk.

## 2.5 Frameworks for assessing information Systems Security Risks

### **2.5.1 Health Insurance Portability and Accountability Act**

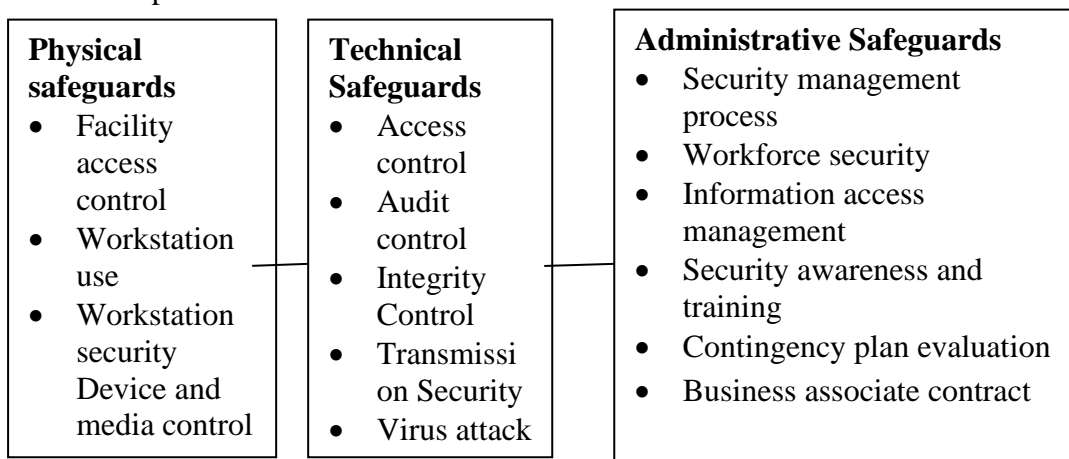
The Health Insurance Portability and Accountability Act (“HIPAA”) was enacted in 1996 by the U.S Department of Health and Human Services in sub chapter C of part 45 of Code of Federal Regulations, to create uniformed formats and rules to covered entities regarding electronic health transmissions that were deemed important. A covered entity is defined by the Act as a health plan, health care clearinghouse, and a health care provider that transmits any health information in electronic form. These rules required the development of specific areas of regulation, including standards for electronic transactions, privacy of individually identifiable health information, national employer identification, security, national provider identification, and proposed enforcement rule. The Act also provides a federal standard of care for Protected Health Information for providers, health insurance plans, and employers.

HIPAA is divided into two main rules – the Privacy Rule and the Security Rule, the privacy rule applies to covered entities and business associates. The HIPAA Privacy

Rule covers any form of protected health information (PHI) unlike the HIPAA Security Rule which only covers electronic protected health information. The privacy rule identifies that public health authorities need to have access to PHI in order to carry out the public mission. In order for this to work the privacy rule allows Covered Entities to disclose protected information, without authority, to legally protected authorities in order to prevent injury and disease.

The HIPAA Security Rule was passed in 2004 by Health and Human Services' Office for Civil Rights (OCR) to ensure that covered entities protect "the confidentiality, integrity, and availability of [electronic Protected Health Information]. Therefore, confidential information should not be disclosed to unauthorized personnel, and entities must prevent any unauthorized alteration and destruction of information, and finally information must be available when demanded .Security risks negatively influence user's acceptance of mobile based services for example location based mobile commerce, security risks have been found to negatively influence users' acceptance of mobile-based services like location-based mobile shopping, health informatics and commerce. Although location based services are a potential means to augment society and businesses, they pose risks linked to sharing personal and location information. Xu, (2019.) The Security Rule allows individuals to access identifiable health information held by covered entities. These rights include ensuring requested information is obtained in a timely fashion and in the specific format requested. DeSalvo et al, (2016) Hazard, L. (2016)

HIPAA outlines the security rule that requires appropriate technical, physical and administrative safeguards to ensure the confidentiality, integrity, and security of electronic protected health information



**Figure 1: Health Insurance Portability and Accountability Act (Source Authorc,2023)**

Because of HIPAA's high-level nature of the requirements which are not being prescriptive, in addition to the absence of a complete risk analysis with just over-reliance on implementing different safeguards, the information protection programs across various organizations incorporating HIPAA have varied. Without valid risk analysis and just complying with HIPAA security rule would result in an approach that does not handle all the threats that a healthcare organization is prone to.

**Pros:** Compliance culture, HIPAA has been instrumental in the creation of a compliance culture in healthcare organizations. For most healthcare organizations HIPAA has become synonymous with security. Healthcare organizations have for long assumed their systems to be secure if it is compliant with HIPAA.

**Cons:** To prevent security violations, HIPAA defines security rule that consists of Standards and Implementations. The implementation controls are indicated as required which create a lot of ambiguity. Since HIPAA is not "certifiable" organizations are required to leverage external assessors and internal resource to perform self-assessment for compliance.

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). The Privacy Rule agree to covered entities who are their business associates to disclose PHI without individual authorization Farmer Y, and Godard B, (2007)

The HIPAA Security Rule is not designed to regulate email and doesn't require HIPAA compliance or encryption. **Compliance & Certification:** Compliance with HIPAA requires organizations to verbally commit to their customers or sign agreements to demonstrate compliance. Besides, organizations will also be required to provide compliance reports to prove compliance. Applicable organizations are required to use the SOC (System and Organization Control) reporting under AICPA (American Institute of Certified Public Accountants) control framework and other TSP's (Trust Services Principles) for reporting HIPAA compliance.

Regulations such as HIPAA allow healthcare provider organizations to disclose protected health information to researchers on grounds that they have obtained consent from patients and approval from an Institutional Review Board (IRB). An estimated 68% of researchers

perceived that HIPAA made medical research highly difficult. However, 25% believed it has increased patients ‘confidentiality. Anecdotal evidence suggests that the new regulatory requirements have had an adverse effect on the conduct of medical research (e.g. Kaiser 2004; 2006; Turner 2002)

An estimated 39% of researchers believed HIPAA had increased research cost by a great deal, due to additional compliance related administrative cost and about 51% of researchers believed HIPAA enforcement lead to inadvertent delays in research. This adverse perspective of HIPAA is reflected in lower adoption rate of health information systems like Electronic Medical Records bolstering the perception that privacy laws may actually have negative effect on the ultimate goals of providing quality care at low cost.

Study by Miller and Tucker (2007) on enactment of state privacy laws regulating health information disclosure across the United States and the adoption rates of EMR, the result shows that hospitals in states with privacy laws were 33% less likely to adopt an EMR system compared to other hospitals. in states with no privacy laws, they found that a hospital ‘s adoption of EMR may increase by 6 percent. In a related study, the result indicated that quality of administrative capabilities in managing access control to healthcare information systems has an impact on administrative cost, user downtime between administrative events, and the ability of users to perform their roles (Hu et al. 2006).

### 2.5.2 International Organization for Standardization 27001 Framework



**Figure 2. International Organization for Standardization 27001 Framework**  
(Source Adopted from ISO/IEC 27001 Information Security Management)



ISO/IEC 27001 published by International Organization for Standardization (ISO) is a collection of Information security management best practices and offers requirements for Information Security Management Systems (ISMS). The standard was published in 2005 and revised in 2013. To provide security controls to protect Personal health information, ISO offers the ISO 27799 standard targeted for the health sector. ISO 27001 can be merged with ISO 27799 standards to address healthcare specific risks. ISO 27001 is a risk-based framework and specifies 114 controls in 14 groups.

**Pros:** Compliance with ISO 27001 illustrates to clients that the organization has put in place best practice information security process. By complying with ISO 27001, organizations can avoid the financial penalties and losses associated with data breaches, comply with business, legal, contractual and regulatory requirements, protect and enhance their credibility and reputations.

**Cons:** ISO/IEC 27001 is industry based and does not completely address some of the healthcare-specific concerns. The requirements provided by ISO are also more generic and less prescriptive

### **2.5.3 HI trust Framework**

According to Clark, et al ... (2018) the increasing digitization of health information and the ever-changing cyber security threat environment has led to some public health data breaches over the past few years. And this trend will likely continue as healthcare organizations struggle to determine and implement a reasonable and appropriate set of safeguards.

Abdulsalam et al...(2019) States that the Health Information Trust Alliance (HITRUST) was formed by a consortium of healthcare organizations in 2007; the main aim was improvements in the state of information security in the industry which are critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges of health information, all of which are necessary to improve the quality of patient care while lowering the cost of healthcare delivery

HITRUST components contain the establishment of a common risk and compliance management framework (CSF); educational and career development; advocacy and

awareness; an assessment and assurance methodology; and a federally recognized cyber Information Sharing and Analysis Organization (ISAO) and supporting initiatives

The HITRUST CSF entails different federal and state regulations in addition to standards and frameworks like COBIT, HIPAA, NIST, and ISO. The CSF provides an elaborate, flexible and prescriptive framework for customizing security control requirements for healthcare organizations of different levels. The CSF uses the ISO/IEC 27001:2005 Information Security Management system as its foundation, mainly with the aim of supporting non-US business associates. The HITRUST CSF is structured similar to ISO 27001 and consists of six main components as illustrated below:

**Control Categories:** has arrange of information protection area such as access control, privacy as defined in ISO 27001

**Control Objectives:** Has sub-topical information protection areas within a control category like Mobile Computing and Teleworking, Openness and Transparency among others

**Controls:** Provides the specific information protection requirements based on ISO 27001 and includes a control reference number, name and specification which describes the control.

**Implementation Requirement Levels:** For each control three levels of a detailed and prescriptive requirement are provided along with associated risk factors.

**Control Requirements:** Detailed and prescriptive requirements contained in an information requirement level that support the control specification

**Standard Mappings:** The specific authoritative source that is directly /indirectly supported by the control requirements, such as NIST SP 800-53 r4 AC-19 or HIPAA 164.502

There are 135 controls that cover security and some privacy-related requirements and 14 controls that cover specific privacy practices in the CSF

**Pros:** Leveraging the HITRUST CSF offers the following benefits

**HIPAA Compliance:** The prescriptive requirement provided by HITRUST CSF would help Medical device companies to respond to the implementation specifications and standards of HIPAA security rule

**Federal Acceptance:** Medical companies that implement the HITRUST CSF have an added advantage of getting recognition from Federal agencies and more likely to receive federal assistance and grants. Implementing the CSF enables the process of getting FDA 510(k) premarket approval

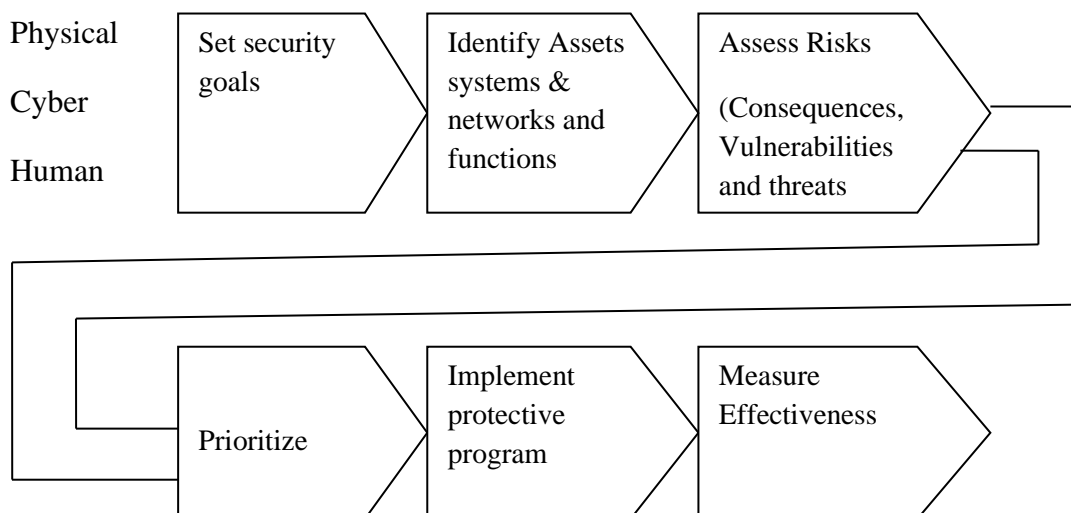
**Limited Liability:** Organizations that have implemented CSF are less liable in the event of a cyber-security incident. Companies also benefit by having to pay less premium for insurance provided if they follow robust security practices

HITRUST framework is broadly adopted across healthcare organization with estimated 80% percent of hospitals and health plans, in addition to many other healthcare institutions and business associates, embrace Common Security Framework. HITRUST is recognized by AICPA and DHHS and annually updated.

**Cons:** The HITRUST CST is not a standard in the league of ISO/IEC 27001:2013. Even though it is internationally adopted, it is yet to be localized outside US English version. Humphreys, E. (2016)

**Compliance & Certification:** HITRUST is a certifiable framework that organizations can use for the creation, storage and exchange of personal health information. The certification process has two phases. First step requires Organizations to perform a self-assessment using HITRUST tool. Based on inputs provided to the tools, a customized assessment is developed to assess the organization's environment with respect to the compliance criteria. Corrective actions from the tools should be incorporated. After which a validated assessment done by third-party certified assessors.

## 2.5.4 national infrastructure protection plan- risk management framework



**Figure 3. Adopted from National Infrastructure Protection Plan- Risk Management framework (source adopted from NIPP)**

The national infrastructure protection plan risk management framework (NNIP-RM) is structured to promote continuous improvement to enhance critical infrastructure protection and key resource protection as shown in Figure 5. and addresses the physical, cyber, and human considerations required for effective implementation of comprehensive programs

The risk management framework is structured to promote continuous improvement to enhance CI/KR protection by focusing activities on efforts to:

**Set security goals:** Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.

**Identify assets, systems, networks, and functions:** Develop an inventory of the assets, systems, and networks, including those located outside the United States, that comprise the Nation’s CI/KR and the critical functionality therein.

**Assess risks:** Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards, known vulnerabilities to various potential attack vectors, and general or specific threat information.

**Prioritize:** Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk, establish priorities based on risk, and determine protection and business continuity initiatives that provide the greatest mitigation of risk. determine protection and business continuity that provide the greatest mitigation of risk.

**Implement protective programs:** Select sector-appropriate protective actions or programs to reduce or manage the risk identified and secure the resources needed to address priorities.

**Measure effectiveness:** Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CI/KR protection program in improving protection, managing risk, and increasing resiliency.

## **2.6 Conceptual Framework**

The existing Frameworks for Assessing Health information security Risks have different challenges ; i) HIPAA ,lacks complete valid risk analysis, not certifiable, safeguarding electronic protected health information only, does not regulate emails ,not using encryption, and commitment on security is verbal.ii) ISO/IEC 27001framework is expensive, requires specific IT budget, special expertise, and more time to apply in public hospitals.iii) NIPP framework is expensive, and uses consequence's assessment which is outside the scope of this study.

In terms of threats and vulnerabilities, as explained by Bernard R, (2020) attacks and threats against hospitals, medical devices and healthcare entities are on the rise. Here, the threat agent utilizes techniques such as phishing, botnets, man-in-the-middle and SQL injections to exploit various vulnerabilities in hospital systems, networks. Nyangaresi VO. (2021). These vulnerabilities may be in software applications, system security procedures, regulatory compliance, policies and procedures. Chuma KG. (2022). The motivation behind these attacks range from financial gains to political gain

To curb these attacks and threats, security frameworks have come up with security control mechanisms that all healthcare facilities need to adopt in order to thwart, detect and minimize vulnerabilities, attacks and threats against their electronic healthcare systems. The three pillars for securing HIS systems comprise of administrative, physical and technical security controls. (Kruse & Ives 2017). The administrative controls may include, staff training, disciplinary actions for violation of policies, rules and procedures for assigning access to HIS, security policies, inventory management, maintenance of audit trails, methods for incident reporting, Risk assessment and data review as well as accountability. Andriole. (2014). On the other hand, physical security controls encompass proper device disposal, device isolation and emergency contingency protocols. Ngethe, N. S. (2021) states that components of physical security measures include Lock and key, secure server rooms, surveillance, and installation of fire alarms and burglary. Khajouei et al., (2017) found out that physical security controls (like lock-and key) reduced chances or exposure of confidential data to unauthorized personnel. In another study by Wanyonyi, E.et al, (2017) On their part, technical security controls include biometrics, access control systems. Nyangaresi VO. (2021). Passwords, encryption, antivirus, firewalls, radio frequency identification (RFID) and Intrusion Detection System (IDS). Lemke, J. (2013). According to Marutha (2019) Healthcare organizations and hospitals subscribe to healthcare legislation's that are regulated by the concerned jurisdiction. These regulations and legislation's offer the groundwork for enhanced and resilient healthcare systems. In this regard, various techniques have been put forward to protect HIS as well as the data exchanged in TMIS.

The conceptual framework was based on the two theories (Control and Auditing theories and Risk management theories). Control and Auditing theory postulates that, organizations need to establish information security control measures which upon implementation, should be followed by conducting auditing procedures to evaluate the performance of control in place. Information security management is considered by many researchers as forming part of control systems. Based on Risk Management Theory, the threats and vulnerabilities regarding information security could be estimated and assessed by doing risk analysis and evaluation. The outcome can aid in planning information security requirements and risk control measures. The aim is to reduce the information security risk to an acceptable level within the organization.

Risk management entails establishing and maintaining information security of an organization

HIPAA framework was implemented in USA, Canada, United Kingdom, Australia. NIPPA has been implemented in USA. While ISO 27001 has been implemented in Japan, China, Germany, Spain. Netherlands, Argentina, Bolivia, Bulgaria, Chile, Colombia and Italy among others (ISO/IEC 27001).

### Conceptual Framework

#### Independent variable

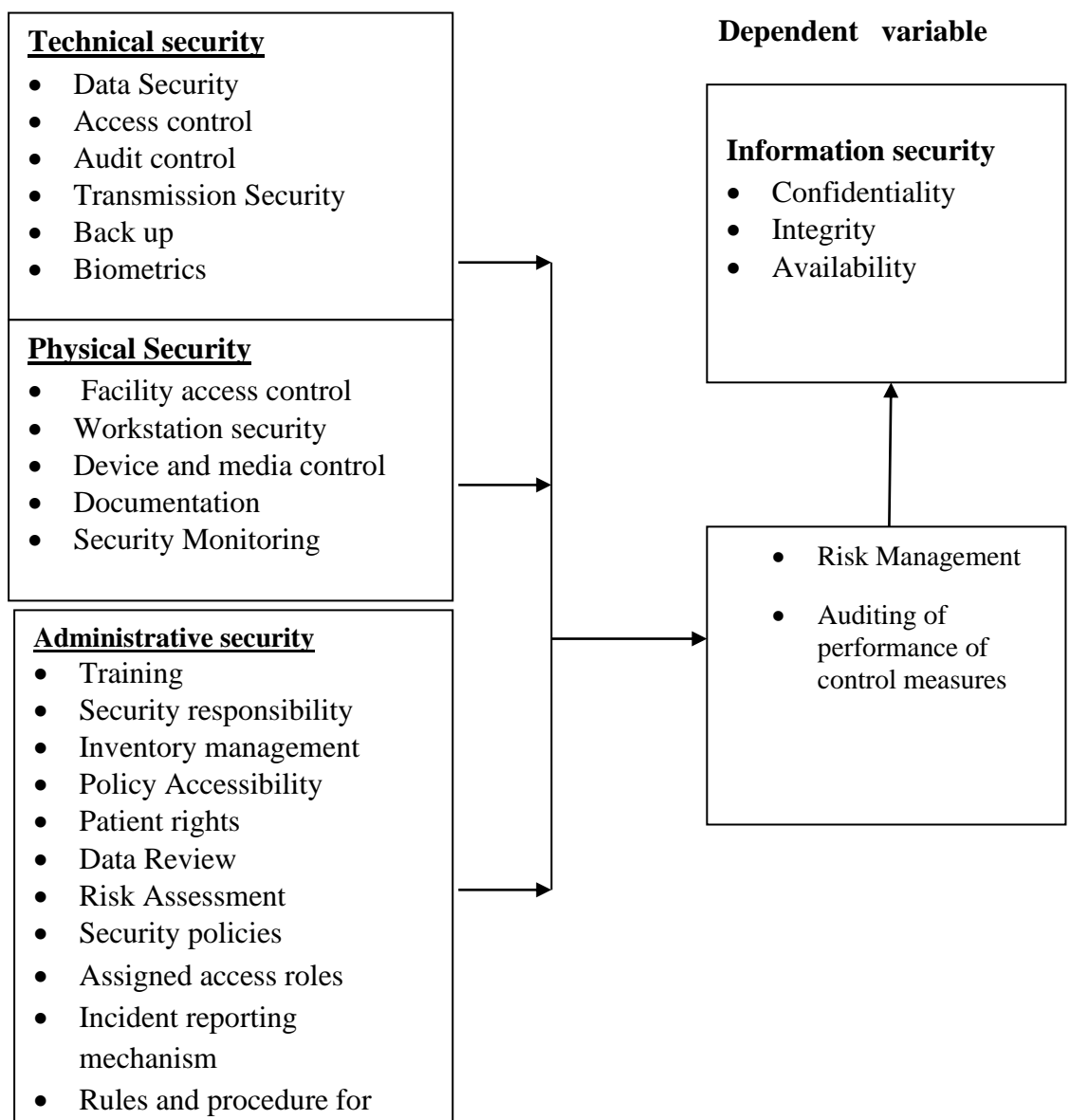


Figure 4: Conceptual Framework

**Source: Researcher, (2023)**

## **2.7 Summary of literature Gaps**

The insecurity of Health Information Systems is derived from a number of factors. Technical Security controls lack or breach of Biometrics, Access controls, pass words, encryptions, antivirus, firewalls, and Radio frequency identification devices. Inadequacies in administrative controls such as training of staff, sanctions, procedures, audit trails, incident reporting, risk assessment, data review. Weaker or lack of physical security controls like proper device disposal, device isolation, emergency contingency protocols, lock and key, secure server rooms, fire walls, burglar proofs and surveillance have all been cited as contributors to HIS security challenges. In addition, the strengths and weaknesses of the following frameworks for assessing HIS Security Risks were assessed: Health insurance Portability and Accountability Act, Health Information Trust Alliance, ISO/IEC 27001, and National Information Protection Plan, the study observed that there are many frameworks but selecting appropriate one is a challenge, the study observed that the four frameworks assessed did not meet desired standards pointing to gap and need to development of an enhanced Framework. HIPAA framework was implemented in USA, Canada, United Kingdom, Australia. NIPPA has been implemented in USA. While ISO 27001 has been implemented in Japan, China, Germany, Spain, Netherlands, Argentina, Bolivia, Bulgaria, Chile, Colombia and Italy among others (ISO/IEC 27001).



## **CHAPTER THREE: RESEARCH METHODOLOGY**

### **3.1 Introduction**

This chapter highlights the methodology used in terms of Location of the study, research design, study Population, data collection instruments and procedures, test tools, data analysis, interpretation and ethical considerations

### **3.2 Location of the Study**

The study was conducted in six public hospitals in Siaya County, which included Siaya County Referral Hospital, Yala Sub County hospital, Bondo Sub County Hospital, Madiany Sub County hospital, mbira Sub County Hospital, Ukwala Sub County Hospital, These six forms 60% of the public hospitals in Siaya County. The choice of Siaya County was based on the data insecurity and loss which was experienced just like other Counties whereby the private patient data are getting accessed in unauthorized people leading to disclosure of private and highly confidential patient information

### **3.3 Research Design**

The study adopted a descriptive cross – sectional research design. Several researchers have recommended descriptive design as the best for such kind of research Levin KA. (2007, Mann CJ. (2003). Grimes DA et al. 2002, Kothari, C. R. 2004, Orodho, J.A. 2005). The study assessed existing HIS security risk, and developed a framework for assessing HIS security and risk

### **3.4 The Target Population**

Population is defined as a composition of elements with similar aspects which the researcher targets to study and draw statistical inference from. Kadam et al...., (2010). A target population is the total sun of individuals of subjects from which a study makes inferences (Blumberg, Cooper & Schindler, 2014). This study targeted six public Hospitals out of the ten public Hospitals based on the following criteria i) must be a public Hospital, ii) must be sub County Public Hospital. The targeted total respondents were 67 but the actual response was 61 which is 91% response rate

The confidence level and precision level were established from the published table 1 below where,  $e$  represents the desired level of precision,  $p$  is the proportion of the population which has the attribute in question, and  $q$  is  $(1 - p)$ . For a confidence level of 95%, the value of  $e = \pm 7\%$ ,

**Table 1: Published Table for Sample size.**

Size of Population	Sample Size (n) for Precision (e) of:		
	±5%	±7%	±10%
100	81	67	51
125	96	78	56
150	110	86	61
175	122	94	64
200	134	101	67
225	144	107	70
250	154	112	72
275	163	117	74
300	172	121	76
325	180	125	77
350	187	129	78
375	194	132	80
400	201	135	81
425	207	138	82
450	212	140	82

Source (Yamane, Taro. 1967.)

### 3.5 Sample Design

Sample size was calculated based on Yamane model (Yamane, 1967) as illustrated below

Mathematically, this model is represented as follows:

$$n = \frac{N}{1 + N(e)^2}$$

Where:

n = Sample size

N = Population size

e = level of Precision or sampling of error at 0.07% with 95% confidence level,)

Given N= 100, then;

$$n = \frac{100}{1 + 100(0.07)^2} = \frac{100}{1 + 100(0.0049)} = \frac{100}{1 + 0.49} = 67 = 67 \text{ participants}$$

**Table 2: Proportionate Stratified Sampling**

<b>Stratum</b>	<b>Target Population</b>	<b>Applied Sample</b>	<b>Actual Response rate</b>
Siaya County Referral Hospital	25	17	15
Yala Sub County Hospital	15	10	9
Bondo Sub County Hospital	20	13	12
Madiany Sub County Hospital	10	7	7
Ukwala Sub County Hospital	15	10	9
Ambira Sub County Hospital	15	10	9
<b>Total</b>	<b>100</b>	<b>67</b>	<b>61</b>

Source: Researcher, (2023)

### **3.6 Data Collection Instruments**

The survey used structured questionnaire with both open and closed ended questions which was administered with an aid of research assistants in Face-to-face interviews with respondents.

### **3.7 Piloting of the Research Instrument**

The data collection instruments were piloted in two hospitals (Uyawi and Rwambwa) which were not involved in the study, the results were used to perfect the instruments and improve the quality output. The reason for choosing these two Hospitals was that they are Sub County Public Hospitals with high workload similar to the six Public Hospitals chosen and they were not to be included in the actual study since the study targeted only six hospitals which had been in operation as sub county Hospital for more than 30 years. Pilot questionnaires were distributed to 20 respondents with same demographic characteristics as the ones in the final respondents selected for convenience purpose

### **3.8 Validity and Reliability**

Reliability concerns the extent to which any measuring procedure yields the same results on repeated trials. Carmines et...al, (1979). The more consistent the results given by repeated measurements, the higher the reliability of the measuring procedure. Validity refers to the degree to which an instrument accurately measures what it intends to measure.

This study focused on two types of validity, first was the content validity which assessed whether the instrument adequately covered all the content that it should

cover with respect to the variables. Content validity was determined by the pilot conducted in two Sub County hospitals, (Rwambwa and Uyawi) that were not included in the survey. The result pointed out the following, the respondent's names not to be included, some questions which were repeated were removed, some questions numbers were missing and were then added. Some questions were leading question and were corrected. The second validity was Face validity which is the extent to which a tool appears to measure what it is supposed to measure. This was confirmed by the expert opinion who in this case were my two supervisors.

### **3.9 Data Collection Procedures.**

The data was collected by distributing questionnaires to respondents. However, interviewees who were busy were given the questionnaires to fill and the questionnaire's collected the following day and they were only 4 participants out of the 61 targeted. The entire period for data collection and review were three weeks.

### **3.10 Data Management and Analysis**

Completed questionnaires were coded and data entry and analysis done using statistical package for social sciences (SPSS V.20). Data was summarized using frequencies, percentage, means and standard deviation. Results are presented in form of charts and tables

### **3.11 Ethical Considerations**

Ethical approval was obtained from Jaramogi Oginga Odinga University of Science and Technology Research and Ethics Committee approval number (ERC7/6/21-26 Vide Ref: JOOUST/DVC-RIO/ERC/E2) and the License to conduct Research was received form National Commission for Science, Technology and Innovation (NACOSTI), License number NASCOSTI/P/21/11562. Permission to conduct the Research in Public health institutions was approved by County Director of Health and Sanitation Siaya, (Vide Ref: CGS/CHD/Research/VOL.IV(105). Participants were informed of their right to participate in the study and the findings were shared with the respondent's upon request in written form.

### **3.12 Summary of Research methodology**

The study was done in Siaya County in Kenya using descriptive cross – sectional research design, ethical approval was sought and obtained from the authorized bodies

(JOOUT, Department of Health and NACOSTI), A total of 61 responded after they were given questionnaires which they answered data were analyzed by SPSS version 24. The targeted population was 80 but managed 61 giving 76.3% achievement, Sample size was determined by Yamane model OF 1967, the data collection tools were tested in two Hospitals (Rwambwa and Uyawwi) and the result used to improve the questionnaires. The actual data was collected from the six Hospitals using questionnaires the analyzed and presented in tables and charts.

## CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSIONS

### 4.1 Introductions

This chapter focuses on the analysis of data, findings and discussions based on the research objectives as follows; to examine existing Health Information Systems security risk, to assess available frameworks for assessing HIS security risk and to develop a framework for assessing HIS security risk

The study targeted a total of 67 respondents but managed 61 respondents giving percentage of 91%. A total 61 questionnaires were completed. Higher proportion of the respondents 36(56.2%) were male and 28(43.8%) were female. More than half 40 (62.5%) were aged between 20 and 30 years old and 22(34.4%) were Health records and information officers. More than half 40 (62.5%) had diploma as highest level of professional training as indicated in table 4.2.1 to 4.4 below.

### 4.2 Demographic Characteristics of the Respondents

The study considered the Demographic Characteristics of the Respondents in terms of Gender, Age, Professional background, Level of Education, and unit of work. These Demographic Characteristics can influence the outcome of information security in a hospital set up hence their consideration.

#### 4.2.1 Table 3: Distribution of Respondents by Gender

Gender	Frequency							Total	Percentage
	SCRH	Bondo	Yala	Madiany	Ukwala	Ambira			
Male	9	8	4	4	6	5	36	56.3	
Female	5	4	6	4	7	2	28	43.7	
Total	14	12	10	8	13	7	64	100	

Source (Researcher, 2021)

Males were the majority Respondents at 56.2% while Females formed 43.7%

#### 4.2.2 Distribution of Respondents by Age

The study sought to establish the respondents age a cross the six Public Hospitals and the Results are indicated in table 3 below

**Table 4 Distribution of Respondents by Age**

Age	SCRH	Bondo	Yala	Madiany	Ukwala	Ambira	Total	Percentage
20---30	9	8	7	5	7	4	40	62.5
31---40	5	4	3	3	6	4	24	37.5
Total	14	12	10	8	13	7	64	100

Source (Researcher, 2021)

From the results in the table 3 above, majority of the respondents 62.5% were between the ages of 20 to 30, while respondents between ages 31 to 40 formed 37.5%

#### 4.2.3 Distribution of Respondents by Professional Background

The study sought to establish the Respondents Professional Background and the result is indicated in table 4

**Table 5 Distribution of Respondents by Professional Background**

Profession	Frequency per Hospital							Total	Percentage
	SCRH	Bondo	Yala	Madiany	Ukwala	Ambira			
<b>Medical Doctor</b>	0	0	1	0	0	0	1	1.6	
<b>Nurse</b>	4	3	3	2	3	1	16	25	
<b>Nutritionist</b>	1	0	0	0	1	0	2	3.1	
<b>Pharmacist</b>	1	2	0	0	1	0	4	6.3	
<b>Health Records and Information Officer</b>	5	4	4	3	3	3	22	34.4	
<b>Clinical Officer</b>	2	3	2	2	3	2	14	21.8	
<b>Environmental Officer</b>	1	0	0	1	2	1	5	7.8	
<b>Total</b>	14	12	10	8	13	7	64	100	

Source (Researcher, 2021)

According to the Research findings majority of the respondents were Health Records and Information Officers at 22(34.4%), followed by Nurses, at 16(25%), Clinical officers at 14(21.8%), Environmental Health at 5(7.8%), then pharmacist at 4 (6.3%), Nutritionists at 3.1%, and last but not least medical doctors at 1.6%. The finding indicates that Health Records and Information Officers are the majority when it

comes to issues with Information security since that is their main responsibility in terms of Health Management Information Systems (HMIS). However, this does not mean they are the majority in terms of cadres

#### 4.2.4 Distribution of Respondents by Level of Education

The study looked into the respondent's level of Education with a view to determine their suitability in answering the questions and the result is stated in table 5 below

**Table 6: Distribution of Respondents by the Level of Education**

Academic Qualification	Frequency per Hospital							Percentage
	SCRH	Bondo	Yala	Madiany	Ukwala	Ambira	Total	
<b>Primary</b>	0	0	0	0	0	0	0	0
<b>Secondary</b>	0	1	1	0	0	0	2	3.1
<b>Certificate</b>	2	3	0	1	4	0	10	15.6
<b>Diploma</b>	9	7	6	5	7	6	40	62.56
<b>undergraduate</b>	3	1	3	2	2	1	12	18.8
<b>Masters</b>	0	0	0	0	0	0	0	0
<b>PHD</b>	0	0	0	0	0	0	0	0
<b>Total</b>	14	12	10	8	13	7	64	100

Source (Researcher, 2021)

According to the Research finding, majority of the respondents 40(62.5%) were diploma holders, followed by Graduate at 12(18.8%), certificate holders were 10(15.6%), and secondary level holders were the least at 2(3.1%). Masters and PHD holders were none the results indicate that the respondents were well educated and in a position to confidently answer the research questions.

#### 4.2.5 Distribution of Respondents by the Department in which they work

The study assessed the respondents by the department where they work to get an equitable representation from different departments and Hospitals which are identified by their MFL codes as SCRH-14080, Yala SCH -14175, Bondo SCH-13507, Ukwala SCH-14156, Ambira SCH-13476 and Madiany SCH-13747. The findings are in table 6



**Table 7 Distribution of respondents by the department where they work**

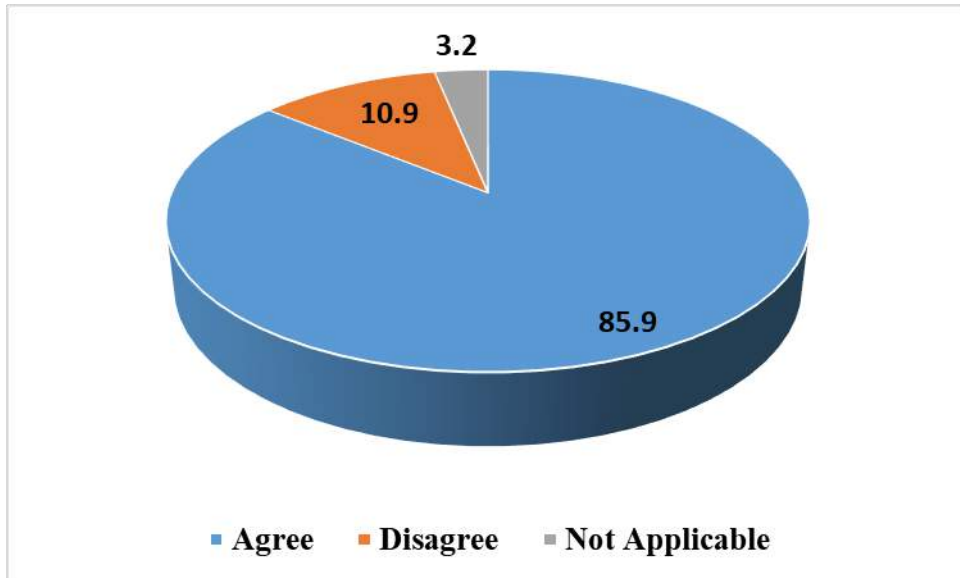
Department	SCR H	Bond o	Yal a	Madia ny	Ukwala a	Ambira a	Total	percentage
Frequency per Hospital								
<b>Comprehensive care Centre</b>	4	2	2	2	5	1	16	25
<b>In patient</b>	1	1	0	0	3	0	5	7.8
<b>Out patient</b>	2	1	5	2	0	1	11	17.2
<b>Public Health</b>	0	1	0	0	1	0	2	3.1
<b>Central Records</b>	1	2	1	3	0	2	9	14.1
<b>Eye Clinic</b>	1	2	0	0	0	0	3	4.7
<b>ICT</b>	1	0	0	0	0	0	1	1.6
<b>Nutrition</b>	1	1	1	0	1	1	5	7.8
<b>Data Room Centre</b>	2	0	0	0	0	0	2	3.1
<b>Pharmacy</b>	1	1	0	1	1	1	5	7.8
<b>Laboratory</b>	0	1	1	0	2	1	5	7.8
<b>Total</b>	14	12	10	8	13	7	64	100

Source (Researcher, 2021)

Majority of the respondents were based at the comprehensive care Centre, 16(25%) followed by the outpatient, 11(17.2%) then Central Medical Records, 9(14%) while Nutrition, Pharmacy, inpatient and medical laboratory had 5 (7.8%) each. Eye clinic had 3(4.7%) Data room Centre and Public Health had 2(3.1%). each and ICT had the least at 1(1.6%) Comprehensive care Centre has the most sensitive information regarding patient level data which needs more confidentiality, and privacy. The median (IQR) years of experience was 2(1.0, 5). The minimum years of experience was 2 months while the highest was 18 years

### **4.3 Objective one: Assessment of Health Information Systems Security Risks**

This section analyzed data on the security of the Health Information system by focusing on the information confidentiality, information integrity and information availability. Majority of the respondents 55(85.9%) agreed to use computer to perform their duties (fig 5)



**Figure 5: Use computer to perform duties**

Among the 55 that use computer to perform their duties, higher proportion used the computers for data entry (94.1%), sending reports (93.8%), report writing (87.2%) and for data analysis (81.4%). Smallest proportion of the respondents (44.8%) used computer for entertainment (fig 6)

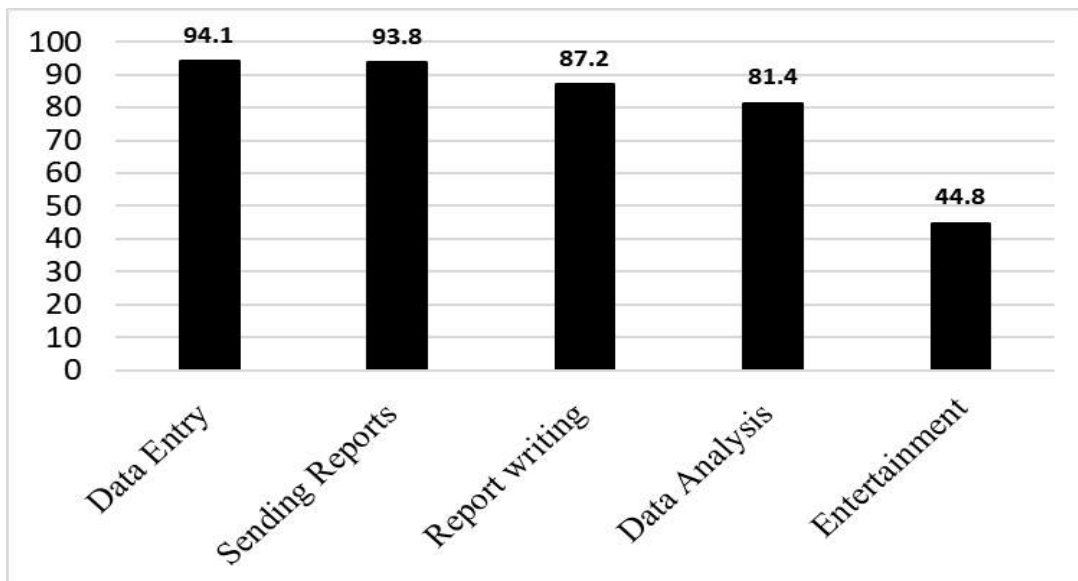


Figure 6: what employees use computer for

#### 4.3.1 Information Confidentiality

The respondents were asked to indicate the level of information confidentiality applied in the six-sub county hospital's Health information systems; the results are presented in table 7 below

**Table 8: Information confidentiality**

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>strongly disagree</b>	<b>Disagree</b>	<b>mean</b>	<b>std Deviatio</b>
staff need a user identifier and password to gain access to a computer	45 (72.6%)	15 (24.2%)	2 (3.2%)			1.3	0.5
computers permitted to be connected to more than one network	29 (47.5%)	23 (37.7%)	3 (4.9%)	1 (1.6%)	5 (8.2%)	1.9	1.2
policies state that staff is personally responsible for protecting paper records, computer workstations, laptop computers associated with confidential information	38 (61.3%)	19 (30.6%)	3 (4.8%)	2 (3.2%)		1.5	0.9
written policy available for ensuring the confidentiality, security of personally identifiable health data	23 (37.1%)	23 (37.1%)	8 (12.9%)	3 (4.8%)	5 (8.1%)	2.1	1.2
The facility is using emails, flash discs, intranet, external hard disk, file transfer protocol, optical media and smart card in transferring electronic data within a site,	25 (40.3%)	23 (37.1%)	7 (11.3%)	2 (3.2%)	5 (8.1%)	2.0	1.2
The facility is using access privileges, encryption ,Antivirus security to protect information during transmission	18 (29.5%)	24 (39.3%)	6 (9.8%)	3 (4.9%)	10 (16.4%)	2.4	1.4
Facility is using Physical measures for protecting patient privacy while collecting information	19 (30.2%)	35 (55.6%)	8 (12.7%)	0 (0%)	1 (1.6%)	1.9	0.8
Physical security control's in place to prevent unauthorized access to buildings and rooms containing personally identifiable	29 (46%)	31 (49.2%)	1 (1.6%)	1 (1.6%)	1 (1.6%)	1.6	0.8

Statement	Strongly Agree	Agree	Neutral	strongly disagree	Disagree	mean	std Deviatio
health data							
<b>Average</b>						<b>1.8</b>	<b>0.1</b>

Source (Researcher,2021)

Majority of the respondents agreed that staff need a user identifier and password to gain access to a computer (96.8%, n= 60), computers permitted to be connected to more than one network (85.2%. n=52), policies state that staff is personally responsible for protecting paper records, computer workstations, laptop computers associated with confidential information (91.9%,,n=59), written policy available for ensuring the confidentiality, security of personally identifiable health data (74.2%,n=46), The facility is using emails, flash discs, intranet, external hard disk, file transfer protocol, optical media and smart card in transferring electronic data within a site, (77.4%,n= 48). The facility is using access privileges, encryption Antivirus security to protect information during transmission, (68.8%, n=42). Facility is using Physical measures for protecting patient privacy while collecting information (85.8%, n= 54) and that Physical security control's in place to prevent unauthorized access to buildings and rooms containing personally identifiable health data (95.2%, n= 57). On average, they agreed with the statements on information confidentiality (mean 1.8, SD 0.1) as indicated in table7.

#### 4.3.2 Data Integrity

The respondents were asked to indicate the extent to which information integrity is applied in the six-sub county hospital's Health information systems. Table 8 presents the findings as follows;

**Table 9: Data Integrity**

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>Strongly Disagree</b>	<b>disagree</b>	<b>Mean</b>	<b>Std Deviation</b>
all persons authorized to access personally identifiable health data trained on the organization's information security policies and procedures	14 (22.2%)	30 (47.6%)	9 (14.3%)	5 (7.9%)	5 (7.9%)	2.3	1.1
Are there clearly defined roles to all persons with authorized access to personally identifiable data?	23 (35.9%)	27 (42.2%)	11 (17.2%)	2 (3.1%)	1 (1.6%)	1.9	0.9
a designated information security manager available at the facility	18 (28.1%)	19 (29.7%)	9 (14.1%)	6 (9.4%)	12 (18.8%)	2.6	1.5
a written description of the information security manager's responsibilities available	7 (10.9%)	17 (28.6%)	18 (28.1%)	8 (12.5%)	14 (21.9%)	3.1	1.3
system to review data accuracy in this facility available	19 (29.7%)	27 (42.2%)	11 (17.2%)	3(4.7%)	4(6.2%)	2.2	1.1
Availability of documented processes for handling data inaccuracies	13 (20.3%)	28 (43.8%)	13 (20.3%)	5 (7.8%)	5 (7.8%)	2.4	1.1

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>Strongly Disagree</b>	<b>disagree</b>	<b>Mean</b>	<b>Std Deviation</b>
electronic systems are monitoring to detect potential or actual security breach	4(6.7%)	20(33.3%)	15(25%)	6(10%)	15(25%)	3.1	1.3
audit logs are created to assist in recording all system transactions	8 (12.7%)	26 (41.3%)	14 (22.2%)	5(7.9%)	10 (15.9%)	2.7	1.3
Data is reviewed frequently for accuracy	23 (35.9%)	29 (45.3%)	6(9.4%)	2(3.1%)	3(4.7%)	2.6	1.4
Audit logs are reviewed frequently	15(23.4%)	18(28.1%)	17(26.6%)	5(7.8%)	9(14.1%)	2.6	1.3
Monitoring of electronic systems to detect potential or actual security breaches done regularly	14(22.2%)	16(25.4%)	16(25.4%)	6(9.5%)	11(17.5%)	2.8	1.4
Are risk assessments conducted in your facility	9(14.9%)	15(23.4%)	17(26.6%)	7(10.9%)	16(25%)	3.1	1.4
risk assessment is conducted monthly	4(6.5%)	13(21%)	17(27.4%)	9(14.5%)	19(30.6%)	3.4	1.3
The following Methods are used to conduct risk assessment Threat identification, vulnerability assessment, Control	7(10.9%)	10(15.6%)	22(34.4%)	8(12.5%)	17(26.6%)	3.3	1.3

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>Strongly Disagree</b>	<b>disagree</b>	<b>Mean</b>	<b>Std Deviation</b>
analysis, Likelihood determination, impact analysis and Risk determination?							
<b>Average</b>						<b>2.6</b>	<b>0.1</b>

Source (Researcher ,2021)

Majority of the respondents agreed that all persons authorized to access personally identifiable health data trained on the organization’s information security policies and procedures (69.8%, n=44), on the other hand availability of clearly defined roles to all persons with authorized access to personally identifiable data (78.1%.n=50), on the availability of a designated information security manager at the facility (57.8%,n= 37 ) meanwhile ,only (39.5% ,n= 24) agreed that a written description of the information security manager’s responsibilities available. Majority of respondents (71.9 % , n= 46) agreed that system to review data accuracy in the facility available, while more than half (64.1%, n= 42) agreed that documented processes for handling data inaccuracies are available, and on whether electronic systems are monitored to detect potential or actual security breach less than half agreed (40%, n= 26). Slightly more than half agreed that audit logs are created to assist in recording all system transactions (54%, n=34). Majority agreed that Data is reviewed frequently for accuracy (81.2%, n= 52), half of the respondent’s agreed that audit logs are reviewed frequently (51.5%, n= 33), while only (38.3%,n=24) agreed that risk assessments conducted in their facilities, (27.5%,n= 17) agreed that risk assessment is conducted monthly in their facilities, and (26.6%,n= 17) agreed that the following Methods are used to conduct risk assessment; threat identification, vulnerability assessment, Control analysis, Likelihood determination, impact analysis and Risk determination. The integrity of data according to the results is low with the least being on risk assessment

### 4.3.3. Information Availability

The study sought to establish the level of information availability across the six sub county hospitals in Siaya County

**Table 10: Information Availability**

Statement	Strongly Agree	Agree	Neutral	Strongly Disagree	disagree	Mean	Std Deviation
Facility has updated inventory of computers and mobile devices containing personally identifiable health data	18 (28.6%)	26 (41.3%)	8 (12.7%)	4 (6.3%)	7 (11.1%)	2.3	1.3
Inventory of computers and mobile devices records are updated regularly	20 (32.3%)	18 (29%)	12 (19.4%)	3 (4.8%)	9 (14.5%)	2.4	1.4
patient data on desktop and laptop are updated frequently	21 (33.3%)	22 (34.9%)	11 (17.5%)	2 (3.2%)	7 (11.1%)	2.2	1.3
Data Confidentiality and Security Policy shared with patients	9(14.1%)	14(21.9%)	13(20.4%)	8(12.5%)	20(31.2%)	3.7	4.0
Facility audit logs are backed up regularly	10(15.9%)	21(33.3%)	17(27%)	3(4.8%)	12(19%)	2.8	1.3
data on desk top and laptop are backed up, regularly	16(25.8%)	24(38.7%)	9(14.5%)	4(6.5%)	9(14.5%)	2.5	1.3
Audit logs are backed up regularly	8(14.8%)	20(37%)	15(27.8%)	4(7.4%)	7(13%)	2.7	1.2
<b>Average</b>						<b>2.6</b>	<b>0.1</b>

Source (Author ,2021)

Majority of the respondent's agreed that Facility has updated inventory of computers and mobile devices containing personally identifiable health data ( 69.9%, n= 44 ).Inventory of computers and mobile devices records are updated regularly



(61.3%,n=38),while the statement that patient data on desktop and laptop are updated frequently (68.2%,n=43) Data Confidentiality and Security Policy shared with patients (36%, n=23) .Facility audit logs are backed up regularly (49.2%, n=43 ) and on whether data on desk top and laptop are backed up, regularly (64.5% n=40), Audit logs are backed up regularly (51% n=28)

**4.4. Objective two: Assessed existing frameworks for assessing Health Information Systems Security Risks**

The study results on assessment of the existing Framework for assessing HIS Security Risks and summarized their strengths, and weaknesses in the table 10 below

**Table 11: Strengths and weaknesses of the existing Frameworks**

Framework	Characteristics	Strengths	Weaknesses
<p>The Health Insurance Portability and Accountability Act (“HIPAA”) was enacted in 1996 by the U.S Department of Health and Human Services in sub chapter C of part 45 of Code of Federal Regulations</p>	<p>-Deals with information security                      - create uniformed formats and rules to covered entities regarding electronic health transmissions                      -Has two rules covering Privacy and security                      - the security rule requires appropriate technical, physical and administrative safeguards to ensure the confidentiality, integrity, and security of electronic protected health information</p>	<p>-The Security rule restricts disclosure of confidential information to unauthorized personnel                      - Enforce compliance culture in healthcare organizations.                      - defines security rule that consists of Standards</p>	<p>- Privacy rule allows Covered Entities to disclose protected information, without authority                      -The Security Rule is not designed to regulate email and doesn’t require compliance or encryption.                      - Rules not prescriptive                      -Lack complete risk analysis                      -Does not handle all the threats in Health care                      -Implementation controls are indicated as required creating ambiguity                      -not certifiable                      - Security Rule specifically focuses on the safeguarding of electronic protected health information</p>

Framework	Characteristics	Strengths	Weaknesses
			<ul style="list-style-type: none"> <li>- Compliance with HIPAA requires organizations to verbally commit to their customers</li> </ul>
<p>-ISO/IEC 27001 published by International Organization for Standardization (ISO, published in 2005 and revised in 2013</p>	<p>-ISO offers the ISO 27799 standard targeted for the health sector</p>	<p>-By complying with ISO 27001, organizations can</p> <ul style="list-style-type: none"> <li>-avoid the financial penalties and losses associated with data breaches,</li> <li>-comply with business, legal, contractual and regulatory requirements,</li> <li>-protect and enhance their credibility and reputations</li> </ul>	<ul style="list-style-type: none"> <li>-The framework is industry based and does not completely address some of the healthcare-specific concerns.</li> <li>- The requirements provided by ISO are also more generic and less prescriptive</li> <li>-Expensive</li> <li>- requires specific IT budget, and special expertise</li> <li>- Not easy to use</li> <li>- lots of time needed to apply requirements to organizational users in regards to the nature, scope and ownership of the public hospitals</li> <li>-Public Health Hospitals are nonprofit making, hence budget may not allow them invest in heavy IT budget.</li> <li>-the resource's required to provide ongoing training and awareness may not be sustainable in the hospital settings</li> </ul>
<p>National Infrastructure Protection Plan- Risk Management framework</p>	<ul style="list-style-type: none"> <li>-Broadly adopted across healthcare organization</li> <li>- Risk Management Framework assess risk in three components</li> <li>Consequences,</li> </ul>	<ul style="list-style-type: none"> <li>- consists of six main components</li> <li>-the current information of each part is looked at against the baseline information captured and analyzed at initial risk assessments to</li> </ul>	<ul style="list-style-type: none"> <li>- estimating potential indirect impacts needs the use of assumptions and more complex variables</li> <li>- An assessment of complete categories of consequence is outside the scope of this study and capabilities available for a given risk</li> </ul>

Framework	Characteristics	Strengths	Weaknesses
	Vulnerabilities and threats	<p>evaluate progress</p> <ul style="list-style-type: none"> <li>-identify key systems, assets, networks, and functions highly in need of focused risk mitigation measures</li> <li>-risk management, principle combining consequence, vulnerability, and threat information aid continuous improvement</li> <li>-process enables a feedback loop, to monitor progress and implement actions to enhance protection and stability of, the physical, cyber, and human components in every process of the risk management frame</li> <li>- consequence is measured as the range of loss that can be expected and in three categories <ul style="list-style-type: none"> <li>-Human Impact,</li> <li>-Economic Impact</li> <li>-Impact on Public</li> <li>-Confidence</li> <li>-Impact on Government</li> <li>Capability</li> </ul> </li> </ul>	<p>analysis</p> <ul style="list-style-type: none"> <li>-this risk management is complex</li> <li>-not easy to understand for people with low IT skills like most of staff in Health sectors whose core mandate is to save life and provide nonprofit services.</li> </ul>

Framework	Characteristics	Strengths	Weaknesses
Data Protection Act,2019 Kenya,(‘THE ACT’)	Safeguarding Personal Information	<p>The Act, provides regulations guiding the following;</p> <ul style="list-style-type: none"> <li>• collection of personal data by data controller or data processor</li> <li>• Duties of data controllers and data processors</li> <li>• Rights of a data subject</li> <li>• Processing of personal data relating to children</li> <li>• Failure to comply with the Act, organization’s may be exposed to hefty fines</li> </ul>	<p>-Data protection lacks definitions, which makes it technologically neutral, but also more difficult to enforce.</p> <p>-Data protection is indiscriminate; it applies to a small business or a club in the same way as it applies to a global conglomerate.</p> <p>-Data networks are global, but data protection is local.</p>

**4.5 Objective three: Develop Enhanced Framework for Assessing HIS Security and Risk**

According to the literature review finding, the frameworks assessed did not meet desired standards leading to development of an enhanced Framework for assessing HIS security Risks in figure 7 below

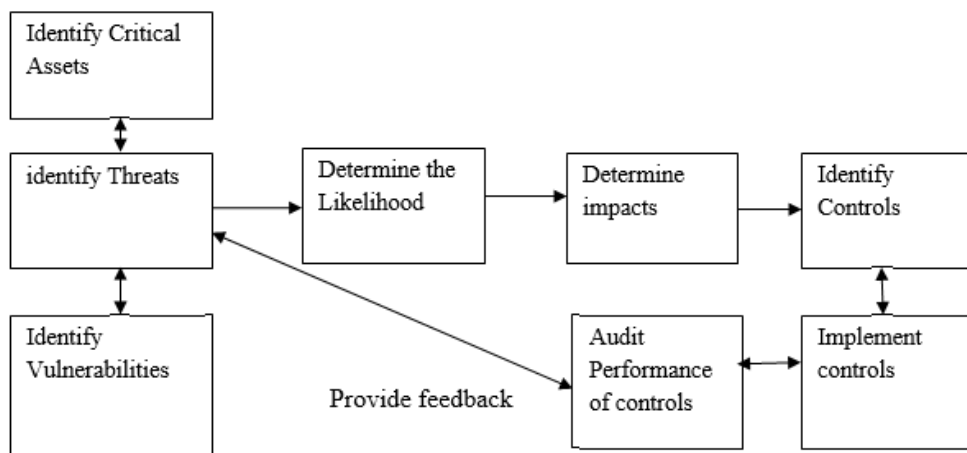


Figure 7 Enhanced Framework for assessing HIS security Risks

The double arrows between identify critical assets and identify threats means the process is continuous same to double arrows between identify threats and identify vulnerabilities, and between identify controls and implement controls. the one way arrows between determine likelihood, impacts, controls indicate sterilized process done on the direction the arrow is indicating

**Figure 7. Proposed Enhanced Framework (Source Researcher ,2022)**

A framework for assessing security risk of an information system must entail comprehensive picture of the available security risk and assist in offering options and alterations to the security measures and controls. Based on this, this study postulates that none of the assessed three frameworks is holistically providing expected outcome. Therefore, the researcher advances the opinion that an enhancement is required which will improve the security risk assessment process, and that enhancement can be made to include three more components which will be added and placed as process (see figure 10). (1) identify likelihood since likelihood of an event exploiting vulnerability is a core measurement in the process of risk assessment which help produces a rating for each asset and (2) determine impacts , Certain impact has the ability to trigger several catastrophic events like the loss of data, damage to laptops and computers , but other impacts may have negligible effect on an institution ,A valid wholesome impact analysis looks into factors such as: impact to the organization’s mission, the systems, and data, besides, this analysis needs to consider the sensitivity and criticality of the data and the system and (3) provide feedback ,Currently, information technology infrastructure is dynamic. So, continuous feedback of security risks and functionality of controls provide accountability of changes to business requirements and priorities, and also new threats and vulnerabilities are detected at an early stage and nipped before its late.

**Identify critical assets**

The information security professional evaluate assets depending on their criticality compared to the whole list of assets available. Assets include databases, applications, hardware, software, People, infrastructure and buildings, the process is cumbersome and needs lots of resources hence only critical assets need to be given priority

**Identify Threats**

The risk assessment process requires institutions to compile a list of threats that could, potentially have an impact on organizational assets. Threats can be considered

as events, actions or inactions, sources, that could lead to the loss or harm of organization assets. The identification of threats needs to be given priority by institutions. Chou, Te-Shun, (2011). A threat may be expected if seen by partner organizations or peers, it may be confirmed or seen before, it may be predicted based on research, it may be anticipated in case of a report, and it may be possible as explained by a source. This analysis may assist in determining the impact likelihood later in the process. The information security threats can be categorized into physical/environmental threats, human threats, and natural disasters Li CT et...el, (2009)

### **Identify Vulnerabilities**

Vulnerabilities are a con founder that make assets capable of being capitalized on by threats. Vulnerability assessment requires that organizations know the specific weaknesses of their assets. To develop a complete list of vulnerabilities, institutions can look at the results of vulnerability assessments, past risk assessments, penetration testing results, security incident data, security metrics audit reports and third party industry events and research. Vulnerability assessment can depend on qualitative and quantitative data to detect its severity. Vulnerabilities can be exposed and easily exploitable that could result in a severe impact however, some vulnerabilities are of no value since they do not cause negative impact if the vulnerability is exploited. Vulnerabilities can be categorized as very low, low, moderate, high and very high, Haugen et...el, (2011)

### **Determine the Likelihood**

The likelihood of an event exploiting vulnerability is a core measurement in the process of risk assessment which help produces a rating for each asset. However, the process can be very subjective and Completing, it relies in historical data in addition to experience of professionals to be exert. The result of this process will lead to a risk rating leading to the amount of energy, money and time, used to control the assets identified from the threat and then assign qualitative values or quantitative values to each threat to enable comparing one event to another, a range of likelihood of threat events range from very low to very high for qualitative, or from 0-100 on a scale for quantitative. Likelihood ratings are used to describe how likely is a successful exploitation of a vulnerability by a given threat. Datta SP, et...el 2010

### **Determine impacts**

Impact is one of the factors used in determining the level of risk to a system. Impact can be measured based on quantitative data and qualitative data in regards to the threat and the asset. Quantitative risk assessments relate to estimating the loss from a monetary point of view using calculations like the Annualized Rate of Occurrence, Single Loss Expectancy, and Annualized Loss Expectancy. Certain impact has the ability to trigger several catastrophic events like the loss of life but other impacts may have negligible effect on an institution. Qualitative risk assessment is subjective hence institutions have to use relative values to assign to the potential impact of an event. Levels typical range from high or critical to low or nonexistent. A valid wholesome impact analysis looks into factors such as: impact to the organization's mission, the systems, and data, besides, this analysis needs to consider the sensitivity and criticality of the data and the system. A tool referred to as FIPS 199 provides a focused consistent process, for rating a system's sensitivity and criticality for the three security domains of availability, confidentiality, and integrity. impact levels are stated using the terms of high, moderate, and low

### **Identify Controls and Audit Performance of controls**

Existing Controls which act as safeguards to protect the system can be identified using a checklist or questionnaire, based on the security need for the system, and also offer guidance on testing security controls. The outcome is applied to reinforce the certainty of the likelihood that a particular threat might successfully exploit a specific vulnerability. Moreira, at... el, (2021).

The aim of identifying existing controls is to reduce the impact of a future event on an asset and reduce duplication of implementing controls that are already in place besides evaluating the effectiveness of the controls security Risk Assessment Methods. The effectiveness of an existing control can be obtained using Historical information to see in case a control in place based on another risk assessment has been helping in reducing the impact of the threat and also identifying weaknesses within the current procedure to enable the control stronger. Hayale, at...el, (2006). The results of audit performance assist in risk-reduction and risk management activities at various levels risk assessment.

### **Provide feedback**

The feedback entails the status of the risk of the system in its current form and provide institutions managers with detailed information for decision risk-based

making regarding resources that should be allocated to the risk mitigation stage. Currently, information technology infrastructure is dynamic. So, continuous feedback of security risks and functionality of controls provide accountability of changes to business requirements and priorities, and also new threats and vulnerabilities are detected at an early stage and precaution taken before its late.

#### **4.6 Discussion of Findings**

##### **4.6.1 Objective one: To examine existing Health Information Systems security risks**

###### **4.6.1.1 Information confidentiality**

The result indicates two perspectives of the practices of information confidentiality in the six sub county hospitals, some practices are bad while others are good as illustrated below. Some practices can lead to breach of confidentiality of information such as connecting computers to more than one network, at (85.2%, n=52) sharing external devices while transferring electronic data from laptops and desktop computers within a site, at (77.4%, n=48) these practices are possible conduits of viral attack, hacking, phishing, stealing of data and even destruction of computers containing the sensitive patient information.

In terms of protecting confidentiality of information, some good practices found in the six sub counties include availability of policies indicating staff responsible for protecting paper records, computer workstations, laptops storing confidential information at (91.9%, n=59) .and written policies available to ensure confidentiality security and privacy of personally identifiable health data at (74.2%.,n=46) Majority of the facilities use access privileges like encryption, antivirus security to protect information during transmission at (68.8%.n=42) .

The practice by staff to use identifier and passwords to gain access to computers at (96.8% n=60) is a good way of securing confidentiality of information stored in computers and laptops. The use of physical measures for protecting patient privacy during data collection at (85.8%, n=54) is one way of promoting confidentiality and privacy and the use of physical security controls to prevent unauthorized access to buildings and rooms containing personally identifiable health data at (95.2%, n=57) is a good strategy to promote confidentiality in the health facilities. In general, the finding on information confidentiality had a mean of 1.8, SD 0.1, overall, the information confidentiality in the six hospitals is good as per the results findings



In a similar finding, a study by Blakely, et al (2002) stated that Risk” must be identified, evaluated, analyzed, treated and reported” and failure in identifying the risks within an institution exposes it to unforeseen consequences with severe outcome”

#### **4.6.2 Data integrity**

The result indicates the status of Data integrity in the six hospitals vary in various aspects some practices are promoting Data integrity, while others do not. On training, (69.8%, n=44) of the respondents agreed that all persons authorized to access personally identifiable health data are trained on the organization’s Data security policies and procedures, while this figure is above average, the remaining 30.2% pose knowledge gap that needs to be checked. on the other hand ,(78.1%,= 50) agreed there are clearly defined roles to all persons with authorized access to personally identifiable data, however, the remaining percentage of 21.9% requires to be given clear roles to improve on Data integrity, Majority of respondents (71.9 %,n= 46) agreed that system to review data accuracy in the facility is available, this is a good practice, however, the accuracy of data is paramount and should be 100% ,in terms of frequency to review data ,Majority agreed that data is reviewed frequently for accuracy with a score of (81.2%,n=52) but on the availability of the documented processes for handling data inaccuracies only (64.1% ,n=42) agreed to the positive. The two variables should score the same since if data is being reviewed frequently, the procedure used in reviewing data should be known to all the staff involved.

The Data integrity status in the six hospitals is performing poorly on the following areas; which are the main areas of focus in this study, (57.8% n=37) agreed that a designated information security manager available at the facility, as a requirement that each facility should have a designated information security Manager. In regards to availability of written description of Data security manager’s responsibilities only (39.5%, n= 24) agreed positively, and on whether electronic systems are monitored to detect potential and/or actual security breach, less than half agreed (40%, n= 26).

The result indicates low score and points to a serious weakness in terms of monitoring the electronic systems which may lead to negative consequences. In terms of creation of audit logs to track all system transactions in the health facility, slightly more than half (54%, n=34), the absence of audit logs is a major weakness since malicious persons may gain access into the system and no one may detect what he/she did in the

system which creates a missed opportunity in suspecting, detecting and tracking malicious actions within electronic systems ,once audit logs are created ,they need to be reviewed in order to aid in trailing any suspicious action ,however only (51.5%,n=33) agreed that audit logs are reviewed frequently this is another weakness detected. In regards to risks assessments which is done with an aim of identifying the threat and vulnerabilities that could impact negatively on confidentiality, integrity and availability of the Information and its system, and setting required control measures to manage the risk. The result indicates that only (38.3%, n=24) agreed that risk assessments conducted in their facilities, this finding points to a major weakness in the fight against Data insecurity and also indication that the Data security within the six hospital is at risk with the low risk assessment conducted, regarding the frequency of conducting risk assessments ,the study findings indicates that (27.5%, n= 17) agreed that risk assessment is conducted monthly in their facilities, and in terms of methods used to conduct risk assessments (26.6%, n= 17) agreed that the following Methods are used to conduct risk assessment; threat identification, vulnerability assessment, Control analysis, Likelihood determination, impact analysis and Risk determination. This finding is in tandem with risk management theory which states that, the threats and vulnerabilities regarding information security could be estimated and assessed by doing risk analysis and evaluation. The outcome can assist in planning information security requirements and risk control measures. The broad aim is to reduce the information security risk to an acceptable level within the institutions.

Similar to the assessment findings, a study by. Wright (1999). states that Risk management comprised establishing and maintaining information security of an institution. By applying information Security Risk management, an organization can protect information in a cost-effective way. According to. Stoneburner.G, et...al. (2002). defines Risk management as the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

#### **4.6.3 Information Availability**

The result illustrates that the availability of information in the six hospitals starting with the statement that facility has updated inventory of computers and mobile devices containing personally identifiable health data at (69.9%, n=44) this score is not good since all the computers and devices with personally identifiable patient

health data needs to be updated in order to track their location and monitor for any potential breach of confidential information in them, and concerning the frequency of updating the inventory of computers and mobile devices (61.3% ,n= 38 ) agreed that it is regularly done, however, the remaining 38.7% is still a bigger gap that needs to be addressed since by updating the inventory regularly can help in identifying any changes that may contribute to potential breach of information. In terms of updating patient data on desktop and laptop, the response was (68.2%, n=43). When some parts of the patient data are updated while other parts are not updated, the availability of data may be compromised since non-updated data can lead to mix up and loss of data. Data Confidentiality and Security Policy shared with patients scored (36%, n=23) this score is poor since Patients should be informed on the confidentiality of their data to win their trust and on the other side the statement that sought to know whether the audit logs are backed up regularly, the response was (51%, n=28) this is not good since backing up information is a secure way of maintaining availability of information in case something interferes with the original storage. On average the information availability in the six facilities had (a mean of 2.6, SD 0.1)

#### **4.6.4 Discussion on existing frameworks**

##### **Objective 2: Assessment of Existing Frameworks for assessing HIS Information Security Risks**

The discussion was based on the study finding on information security framework's ability to provide security of information as required

#### **HIPAA**

HIPAA was enacted in 1996 and is divided into two main rules – the Privacy Rule and the Security Rule, the privacy rule applies to covered entities and business associates. The HIPAA Privacy Rule covers any form of protected health information (PHI) unlike the HIPAA Security Rule which only covers electronic protected health information. The HIPAA Security Rule ensure that covered entities protect “the confidentiality, integrity, and availability of electronic Protected Health Information. Therefore, confidential information should not be disclosed to unauthorized personnel, and entities must prevent any unauthorized alteration and destruction of information, and finally information must be available when demanded for.

Despite the benefits of HIPAA to organizations, there are drawbacks which make it not the better option. HIPAA requirements are not being prescriptive, and lack complete risk analysis with just over-reliance on implementing different safeguards,

without valid risk analysis and just complying with HIPAA security rule would result in an approach that does not handle all the threats that a healthcare organization is prone to. The implementation controls are indicated as required which create a lot of ambiguity. Since HIPAA is not “certifiable” organizations are required to leverage external assessors and internal resource to perform self-assessment for compliance. The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). Wood, (2019). Yet this research is looking at Hospitals with both electronic and paper-based systems. The HIPAA Security Rule is not designed to regulate email and doesn’t require HIPAA compliance or encryption. Compliance with HIPAA requires organizations to verbally commit to their customers or sign agreements to demonstrate compliance

### **ISO/IEC 27001 Framework**

ISO/IEC 27001 provides many benefits to organizations as stated below, however, the Frameworks disadvantages such as being expensive, the fact that it requires specific IT budget, special expertise, in addition to lack of knowledge, not easy to use, time required to apply them to organizational users in regards to the nature, scope and ownership of the public hospitals and the fact that public Health Hospitals are nonprofit making may not allow them invest in heavy IT budget. Besides the resource’s required to provide ongoing training and awareness may not be sustainable in the hospital settings

Among the ISO/IEC 27001 benefits highlighted; include benefits to business in that the framework provides a common understanding, best practices, state of the art, protection of businesses, Technical agreements, systems interoperability, worldwide technology compatibility, Efficiency and customer satisfaction and that it requires commitment

### **National Infrastructure Protection Plan- Risk Management framework**

The main focus of NIPP-RM framework is to identify key systems, assets, networks, and functions highly in need of focused risk mitigation measures this risk management, principle combining consequence, vulnerability, and threat information aid continuous improvement. The current information of each part is looked at against the baseline information captured and analyzed at initial risk assessments to evaluate progress. This process enables a feedback loop, to monitor progress and implement actions to enhance protection and stability of, the physical, cyber, and human

components in every process of the risk management frame. **The NIPP:** Risk Management Framework assess risk in three components Consequences, Vulnerabilities and threats. **Consequence:** consequence is measured as the range of loss that can be expected. And can be summarized into four main categories i) **Human Impact:** Effect on human life and physical wellbeing ii) **Economic Impact:** Direct and indirect effects on the economy iii) **Impact on Public Confidence:** Effect on public morale and confidence in national economic and political institutions; and iv) **Impact on Government Capability:** Effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions

A whole consequence assessment takes into consideration economic, psychological, public health and safety, and government impacts; however, estimating potential indirect impacts needs the use of assumptions and more complex variables. An assessment of complete categories of consequence is outside the scope and capabilities available for a given risk analysis. At a minimum, assessments should focus on the two most fundamental impacts: the human and the most relevant direct economic impact.

Assets, systems, and networks include the following elements: Cyber—electronic information and communications systems, Physical—tangible property; and the information within them; and Human—critical knowledge of functions and people uniquely susceptible to attack

Based on the above reasons, this NIPP-Risk management is not simple and neither is it easy to understand for people with low IT skills like most of staff in Health sectors whose core mandate is to save life and provide nonprofit services.

#### **THE DATA PROTECTION ACT 2019, KENYA (“THE ACT”)**

Data protection is the process of safeguarding personal information, in accordance with a set of principles laid down by law. The framework has developed mainly in response to technological advances which increase the collection, holding and dissemination of personal information as well as surveillance of people. It is essential for data controllers or processors to familiarize themselves with the provisions of the Act and to develop policies and systems that are compliant with the requirements of the Act. Many organizations will require a Data Protection Officer whose main

function will be to ensure compliance with the Act, failure to which organizations may be exposed to hefty fines. Data controllers and processors are required to process data lawfully whilst minimize its collection and ensuring that there are sufficient safeguards in place to protect personal data. Bentotahewa, et ...el, (2021).

The Act, provides regulations guiding the following;

- collection of personal data by data controller or data processor
- Duties of data controllers and data processors
- Rights of a data subject
- Processing of personal data relating to children
- Failure to comply with the Act, organization’s may be exposed to hefty fines

#### 4.6.5 Summary of the assessment of the three Information Security Frameworks

**Table 12: Characteristics, strengths and weaknesses of reviewed Existing Frameworks for assessing HIS Security risks**

Framework	Characteristics	Strengths	Weaknesses
The Health Insurance Portability and Accountability Act (“HIPAA”) was enacted in 1996 by the U.S Department of Health and Human Services in sub chapter C of part 45 of Code of Federal Regulations	-Deals with information security - create uniformed formats and rules to covered entities regarding electronic health transmissions -Has two rules covering Privacy and security - the security rule requires appropriate technical, physical and administrative safeguards to ensure the confidentiality, integrity, and security of electronic protected health information	-The Security rule restricts disclosure of confidential information to unauthorized personnel  - Enforce compliance culture in healthcare organizations. - defines security rule that consists of Standards	- Privacy rule allows Covered Entities to disclose protected information, without authority  -The Security Rule is not designed to regulate email and doesn’t require compliance or encryption.  - Rules not prescriptive  -Lack complete risk analysis  -Does not handle all the threats in Health care  -Implementation controls are indicated as required creating ambiguity -not certifiable - Security Rule

			<p>specifically focuses on the safeguarding of electronic protected health information</p> <ul style="list-style-type: none"> <li>- Compliance with HIPAA requires organizations to verbally commit to their customers</li> </ul>
<p>-ISO/IEC 27001 published by International Organization for Standardization (ISO, published in 2005 and revised in 2013</p>	<p>-ISO offers the ISO 27799 standard targeted for the health sector</p>	<p>-By complying with ISO 27001, organizations can</p> <ul style="list-style-type: none"> <li>-avoid the financial penalties and losses associated with data breaches,</li> <li>-comply with business, legal, contractual and regulatory requirements,</li> <li>-protect and enhance their credibility and reputations</li> </ul>	<p>-The framework is industry based and does not completely address some of the healthcare-specific concerns.</p> <ul style="list-style-type: none"> <li>- The requirements provided by ISO are also more generic and less prescriptive</li> <li>-Expensive</li> <li>- requires specific IT budget, and special expertise</li> <li>- Not easy to use</li> <li>- lots of time needed to apply requirements to organizational users in regards to the nature, scope and ownership of the public hospitals</li> <li>-Public Health Hospitals are nonprofit making, hence budget may not allow them invest in heavy IT budget.</li> <li>-the resource's required to provide ongoing training and awareness may not be sustainable in the hospital settings</li> </ul>

<p>National Infrastructure Protection Plan- Risk Management framework</p>	<p>-Broadly adopted across healthcare organization  - Risk Management Framework assess risk in three components  Consequences, Vulnerabilities and threats</p>	<p>- consists of six main components  -the current information of each part is looked at against the baseline information captured and analyzed at initial risk assessments to evaluate progress  -identify key systems, assets, networks, and functions highly in need of focused risk mitigation measures  -risk management, principle combining consequence, vulnerability, and threat information aid continuous improvement  -process enables a feedback loop, to monitor progress and implement actions to enhance protection and stability of, the physical, cyber, and human components in every process of the risk management frame  - consequence is measured as the range of loss that can be expected and in three categories  -Human Impact,  -Economic Impact  -Impact on Public  -Confidence  -Impact on Government  Capability</p>	<p>- estimating potential indirect impacts needs the use of assumptions and more complex variables    - An assessment of complete categories of consequence is outside the scope of this study and capabilities available for a given risk analysis    -this risk management is complex    -not easy to understand for people with low IT skills like most of staff in Health sectors whose core mandate is to save life and provide nonprofit services.</p>
---	--	---	--



<p>ata Protection Act,2019 Kenya,('THE ACT')</p>	<p>Safeguarding Personal Information</p>	<p>The Act, provides regulations guiding the following;</p> <ul style="list-style-type: none"> <li>• collection of personal data by data controller or data processor</li> <li>• Duties of data controllers and data processors</li> <li>• Rights of a data subject</li> <li>• Processing of personal data relating to children</li> <li>• Failure to comply with the Act, organization's may be exposed to hefty fines</li> </ul>	<p>-Data protection lacks definitions, which makes it technologically neutral, but also more difficult to enforce.          -Data protection is indiscriminate; it applies to a small business or a club in the same way as it applies to a global conglomerate.          -Data networks are global, but data protection is local.</p>
--	--	--	--

**Drawbacks of each framework**

**i) HIPAA.**

HIPAA requirements are not prescriptive

lack complete risk analysis

just over-reliance on implementing different safeguards,

lack valid risk analysis and approach does not handle all the threats that a healthcare organization is prone to.

The implementation controls are indicated as required which create a lot of ambiguity.

HIPAA is not “certifiable”. Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). And does not include paper Health Information contrary to this study’s aim. The Security Rule is not designed to regulate email and doesn’t require compliance or encryption. Compliance with HIPAA requires organizations to verbally commit to their customers or sign agreements to demonstrate compliance

### **ii) ISO/IEC 27001 Framework**

Expensive,

requires specific IT budget, and special expertise,

Not easy to use, due time required to apply requirements to organizational users in regards to the nature, scope and ownership of the public hospitals

Public Health Hospitals are nonprofit making, hence budget may not allow them invest in heavy IT budget.

The resource's required to provide ongoing training and awareness may not be sustainable in the hospital settings

### **iii) NIPP-RM**

The framework focuses on consequence which, describes the effects an institutions misfortune would have on others who are dependent on it

estimating potential indirect impacts needs the use of assumptions and more complex variables. Hence unreliable and expensive for small institutions

An assessment of complete categories of consequence is outside the scope and capabilities available for a given risk analysis.

At a bare minimum, assessments need to look at the two most fundamental impacts: the human and the key relevant direct economic impact.

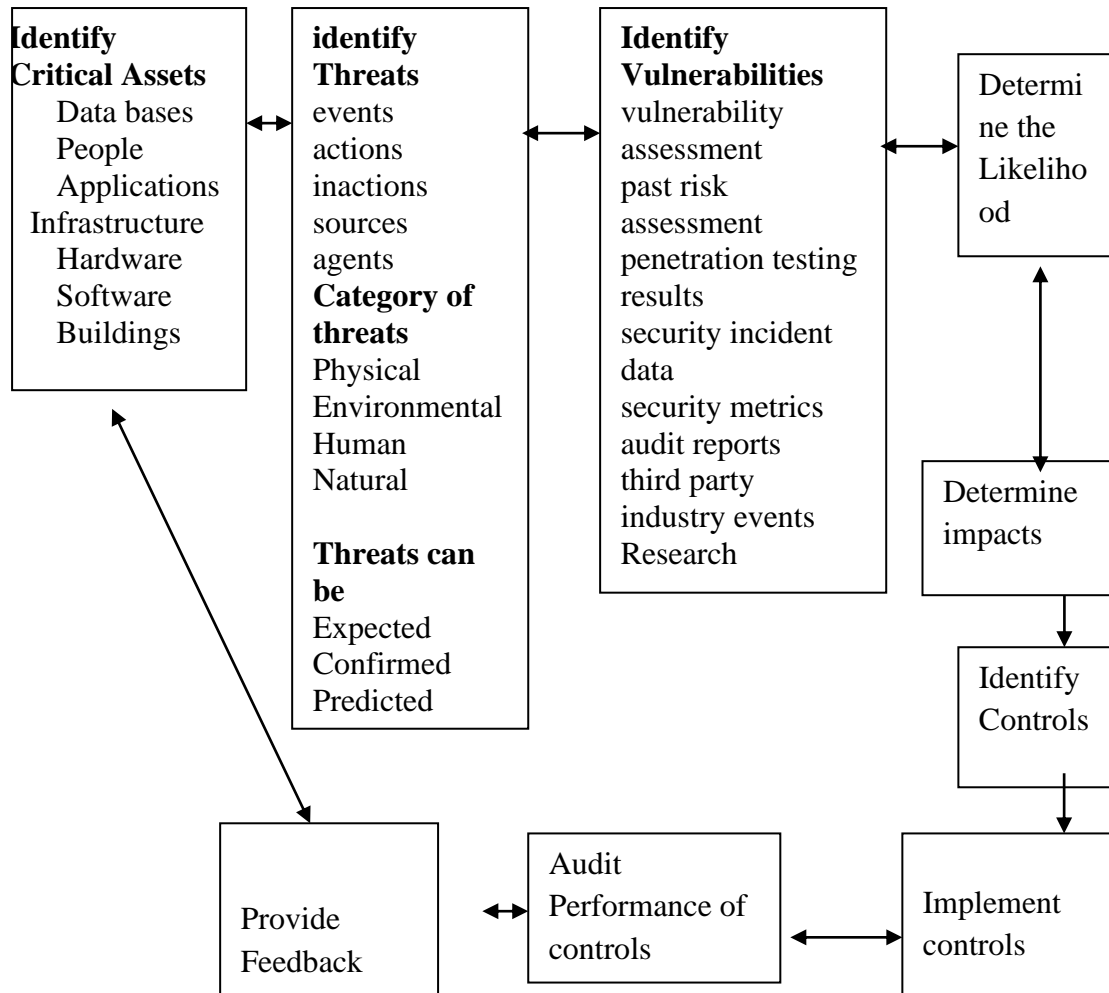
Based on the above reasons, this NIPP-Risk management is not simple and neither is it easy to understand for people with low IT skills like most of staff in Health sectors whose core mandate is to save life and provide nonprofit services.

The framework start with set security goals, should start with identify threats, and the second phase which identify assets, systems, network and functions should start with identify vulnerabilities then the third phase starting with assess risks, Consequences, Vulnerabilities and threats need to start with identify assets then followed by determine the impacts and the likely hood of the threat

having carefully, assessed the three Frameworks (HIPAA, ISO/IEC 27001 and NIPP-RM), non meets the standards desired for a simple, easy to use and re-adjustable framework that covers the most important components of an information security requirement that follow the right procedure and addresses the most fundamental

elements of a framework, and that is why this study proposes an enhanced framework in figure 8.

**4.6.5: Developed Enhanced Framework for assessing HIS Security Risks**  
**Objective three: Developed Enhanced Framework for assessing HIS Information Security Risks**



**Figure 8: proposed enhanced framework (Source Researcher ,2023)**

The double arrows between identify critical assets and identify threats as well as identify threats and identify vulnerabilities show that the process is continuous process. The arrow after determine impacts, identify controls and implement controls indicate serialized activity while the double arrows between audit controls, feedback and identify critical controls indicate continuous process

**Identify critical assets**

Assets should include databases, applications, hardware, software, People, infrastructure and buildings, since the process is cumbersome and expensive only critical assets need to be given priority

**Identify Threats**

The risk assessment process requires institutions to compile a list of threats that could, potentially have an impact on organizational assets.

**Identify Vulnerabilities**

Vulnerabilities make assets capable of being capitalized on by threats. Vulnerability assessment requires that organizations know the specific weaknesses of their assets. The Vulnerability assessment can depend on qualitative and quantitative data to detect its severity.

**Determine the Likelihood**

The likelihood of an event exploiting vulnerability is a core measurement in the process of risk assessment which help produces a rating for each asset. The risk rating leads to identification of the amount of energy, money and time, used to control the assets identified threat and then assign qualitative values or quantitative values to each threat to enable comparing one event to another

**Determine impacts**

Impact is one of the factors used in determining the level of risk to a system. Impact can be measured based on quantitative data and qualitative data in regards to the threat and the asset. data and the system.

**Identify Controls and Audit Performance of controls**

Existing Controls which act as safeguards to protect the system can be identified using a checklist or questionnaire, based on the security need for the system, and also offer guidance on testing security controls.

**Provide feedback**

The feedback entails the status of the risk of the system in its current form and provide institutions managers with detailed information for decision risk-based making regarding resources that should be allocated to the risk mitigation stage.

#### **4.6.6. SUMMARY OF DATA ANALYSIS, RESULTS AND DISCUSSIONS**

Findings of the results and discussions were based on analysis of objectives one, two and three. A total of 61 respondents completed and returned their questionnaires, out of which 56% were males and majority were aged between 20 to 30 years with majority having Diploma their highest academic level and certificate were the least at 3.1%. In terms of cadres Health Records and Information were the majority at 34%. The study found out that 80% of the respondent's use computer to do their work, and out of that, 94% of respondent's use computers for data entry .in terms of the department of work, majority were from comprehensive care Centre at 25% while the least were from ICT at 1.6%. Objective one assessed the Risks to information confidentiality and the results indicated it was good with a mean of 1.8 and std deviation of 0.1. on the other side, information integrity was poor, as there was no designated information security officer in most the facilities, only a few Hospitals have audits logs only created in few facilities at 54%,38.3% while 27 % said risk assessments is conducted. In terms of information availability, most hospitals have access to information when required. The objective three assessed the existing Frameworks for assessing HIS security Risks and the following were assessed Health Insurance Portability and Accountability Act, drawbacks were non-prescriptive ,lack complete risk analysis, no valid risk analysis ,not certifiable ,focuses only on electronic data .ISOS 27001 Framework was found to be expensive, require special IT skills ,not easy to use, not sustainable The National Infrastructure Protection Plan Risk Management is difficult to use, complex , and not easy to understand .The three Frameworks assessed did not meet the requirement needed of a good framework leading to the development of an enhanced Framework .The developed enhanced Framework had in addition to what the other Frameworks did not have like, Identify critical assets ,identify threats ,identify vulnerabilities ,determine likelihood ,determine impacts ,audit controls implement controls, and provide feedback.

## **CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS**

### **5.1 Introduction**

This chapter presents the summary of the study findings, conclusion and recommendations drawn from the Research findings.

### **5.2 Summary of the Findings**

#### **5.2.1 Objective one: Assessing Health Information Systems Security Risks**

The study sought to examine existing Health Information Systems security risk, to assess available frameworks for assessing HIS security risk, and to develop an enhanced framework for assessing HIS security risk. The study, revealed that Information Confidentiality, in the six sub county hospitals is good and has good practices which promote confidentiality of information and bad practices that facilitate breach of confidentiality. Practices promoting confidentiality of information included use of identifiers and passwords in laptops and desk top computers at 96.8% this was followed by availability of physical security controls to protect unauthorized access to buildings and rooms with Health identifiable data (Patient level data) at 95.2% this was then followed by availability of policies that state staff are responsible for protection of information confidentiality at 91.9%, the study also revealed that availability of physical measures to protect patient privacy during data collection at 85.8% ,the other good practices to protect confidentiality was on availability of written policy to ensure confidentiality and privacy of patient level data at 74.2% the last practice to safeguard confidentiality was on use of access privileges like encryption, and Antivirus to protect information during transmissions at 68.8%

The finding showed that among the practices that could contribute breach to information confidentiality, connecting computers to more than one network, was leading at 85.2%, followed by sharing of external devices while transferring electronic data at 77.4%

The study findings showed that the second component of the CIA Triad which is integrity of the information in the six sub county hospital's is poor. The positive side indicates availability of systems to review data accuracy at 71.9% and that data is reviewed frequently at 81.2%, these two are good practices that promote information integrity. However, the study findings indicate negative practices that reduce information integrity like availability of written description of information security manager's responsibility at 39.5% this shows that 60.5% of the hospital's do not have

written responsibilities for security manager ,and monitoring of electronic systems to detect potential and/or actual security breaches was at 40% this is bad practice because without monitoring security potential or actual breaches ,the information systems are exposed to insecurity with bad consequences. In a similar study, the findings indicated that Currently, information systems and computers are the noble assets in each institution that must be safe guarded due to the value of information. All institutions are required to adopt an information security risk management approach to be able to identify the potential threats and risks to the information security, Wilkinson, (October,2013)

The finding indicates that creation of audit logs to track all systems transactions scored 54% and on how frequent is the audit logs reviewed stood at 51.5% Audit logs are vital resources that indicate the current state of the systems and user activities and are used for cyber forensics and maintenance. Audit logs are the sole evidence that can aid in tracking traces of malicious activities and also troubleshooting a system malfunctions. Accountable audit logs can provide better level of trust for service providers as well as service clients. In trusted computing systems evaluation criteria (Qiu et al., 1985), security requirements of audit logs are described as audit data must be protected from modification and unauthorized destruction to permit detection and after-the-fact investigation of security violations. Audit logs play very important roles which include Functionality and performance of information systems such as unit devices can be monitored and explored by analyzing the logs generated by interconnected devices. All operations are recorded in audit logs. Activities of insiders and local administrators along with other users can also be determined by these logs. In system security perspective, malicious activity can also be detected by analyzing these logs, therefore, security, safety, and integrity of audit logs are vital. Audit logs also aid administrators to counter information security issues, forensics is mostly dependent on these logs and such resources play vital part in information systems security

The Study finding on the Risk Assessment in all the six public Hospitals scored the lowest in all the variables assessed. like on whether Risk Assessment is conducted in the hospitals scored 38.3% and whether the Risk Assessment is conducted monthly stood at 27.5% the assessment further looked into whether the Risk Assessment is done using the following methods (threat identification, vulnerability assessment, likelihood determination, impact analysis and Risk determination) scored 26.6%.

According to a similar study on cyber risk there are several methods for assessing information security risks and most of them include identifying threats and vulnerabilities, analyzing the probability and impact associated with the known threats, and ultimately, prioritizing the risks to determine the appropriate level of training and controls necessary for effective mitigation, Wilkinson C et al, (2013). In a similar study, the finding indicated that analysis and assessment of information security risks is a key component of an integrated approach to information security. Risk, in a broader concept, is the probability of an event that details certain losses. Information security risk is the potential probability of using vulnerabilities of an asset or group of assets as a specific threat to damage the organization (ISO/IEC 27005:2018). The purpose of information security risk assessment is to evaluate the risk factors and arrive at the best decision on risk management. Risk factors are the major parameters considered when assessing risks. The seven parameters are asset, threat losses, amount of average annual losses, vulnerability, return on investment and control mechanism.

Information security risk analysis can be divided into two types: qualitative and quantitative for qualitative risk assessment, the main focus is on the likelihood of an event. These likelihoods are obtained from analyzing the threats and vulnerabilities, and then generating a qualitative or quantitative value for the assets that may be affected (impact):  $Risk = Threat \times Vulnerability \times Impact$  (1) where  $Threat \times Vulnerability$  is likelihood

The finding on the last component of the CIA Triad which is availability of information, scored above average as per the results of the study, to start with the areas with the highest score like availability of updated inventory of computers and mobile devices containing patient data level (identifiable data) scored 69.9%, followed by regular updates of inventory of computers and mobile devices at 61.3% meanwhile updating of patient data on laptops and desk tops scored 68.2% .However, assessment on whether data confidentiality and security policy shared with Patients scored 36% and assessment on whether regular back up of audited logs is done scored 51% . Accountable audit logs can offer excellent level of trust for service providers and service clients. In trusted computing systems evaluation criteria (Qiu et al., 1985), security requirements of audit logs are stated as audit data should be secured from unauthorized destruction and modification to allow detection and after-the-fact



investigation of security breaches. Availability of information can be provided by redundant resources. Data Security can be provided by a secure and legitimate authentication and authorization mechanism for remote users

Performance and Functionality of information systems and their interconnected devices can be closely monitored and assessed by analyzing the logs generated by these interconnected devices. All service operations are recorded in audit logs. Activities of insiders and local administrators in addition to other users can also be determined by these logs. In system security point of view, any malicious activity can be identified by analyzing these logs, therefore, security, safety, and integrity of these logs are very crucial. The logs aid administrators to counter information security issues, forensics is majorly dependent on these logs and such resources provide key roles in information systems security.

### **5.2.2 Objective two; Assessing existing Frameworks for assessing HIS Security Risks**

The finding on assessment of existing security frameworks revealed the strengths and weaknesses of each security framework as follows,

- a) Health Insurance portability and accountability Act (HIPAA) Framework has the following weaknesses that makes it not suitable for assessing information security, i) the requirements are not prescriptive, ii) lack complete valid risk analysis, iii) HIPAA framework is not certifiable, iv) it's security rule only concentrates on safe guarding electronic protected Health information, while this study focused on both electronic and paper based ,v) the security rule component is not designed to regulate emails ,and doesn't require encryption. vi) HIPAA framework simply requires organizations to verbally commit to their customers and/or sign agreements to demonstrate compliance
- b) The ISO/IEC 27001 Framework. this framework is a collection of best practices, however, it has the following drawbacks i) it is expensive, ii) requires specific IT budget and special expertise to use, hence iii) difficult to use, iv) the framework requires more time to apply in regards to the nature, scope, and ownership

by public hospital v) The framework is therefore not fit for public hospitals which are not for profit making

- c) National Infrastructure Protection Plan (NIPP): The study findings revealed the weakness of NIPP framework has the followings, i) the framework uses Consequence assessment which is the process of describing and quantifying the relationship between exposures to a risk agent and the adverse public health safety, environmental, economic, psychological and Government impact consequences that result from such exposures. This process makes the framework to be expensive. ii) estimating indirect impacts needs the use of assumptions and more complex variables iii) assessment of complete categories of consequences is outside the scope and capabilities of a given risk analysis

### **5.2.3 Developed Enhanced Framework for assessing HIS security Risks**

The three frameworks (HIPAA, ISO/IEC 27001, and NIPP) assessed above, lack the essential components of what an effective framework to assess information security risks should have which led to the development of proposed enhanced framework with the following essential components required; i) identify critical assets (Database, People, applications, infrastructure, hardware, software and buildings) ii) Identify threats (events, actions, inaction's, sources, agents ) these threats can lead to harm and/or loss of an asset. The threats are categorized into Physical, Environmental, Human and Natural) and threats can be expected, confirmed, predicted, anticipated and/or possible, iii) identify vulnerabilities; Vulnerabilities make assets capable of being capitalized on by the threats hence organization's must know specific weaknesses of their assets, by developing list of vulnerabilities through (vulnerability assessment, past risk assessment, penetration testing results, security incident data, security metrics audit reports ,third party industry events and research),vulnerabilities can be categorized as very low, low, moderate ,high and very high),iv) Determine the likelihood (likelihood of an event exploiting vulnerabilities ,the result lead to risk rating which is used to estimating amount of energy ,money, and time used to control the assets, then assign qualitative values to each of threat and likelihood of an event range from very low to very high for qualitative data while 0-100 on a scale of quantitative data .Likelihood rating is used to describe how likely is a successful exploitation of a vulnerability by a given threat v) Determine impacts ;impacts

determine the level of risk to a system vi) Identify the controls and audit performance and lastly vii) Provide feedback

The study findings revealed that all organization's need information to operate and disruption to information lead to a security breach of an organization's operations. The increasing digitization of health information and the ever-changing cyber security threat environment has led to some public health data breaches over the past few years. As a result, all institutions are required to adopt an information security risk management strategy in order to identify the probable threats and risks to the information security

As information security become increasingly important to the continued success for businesses, majority of organizations are searching for an appropriate security framework (Yhan, 2005). Information security framework is defined as a comprehensive security model that safeguards the entire security of information. The model includes people, process, and business strategies of an organization in which the need for information security is emphasized.

### **5.3 Conclusion**

Based on the study findings, it is concluded that security of health information systems in the six public Hospitals is in place and among the three CIA Triad: protection of **information confidentiality** is leading based on i) availability of policies indicating that staff are responsible for protecting paper records, computer work stations, and laptops with data .ii) Written policies available to ensure confidentiality security of personally identifiable health data iii) use of access privileges like encryption, antivirus to protect information during transmission ,iv) use of identifier and passwords to gain access to computers v) the use of physical security controls to prevent unauthorized access to buildings and rooms containing personally identifiable health data . In general, the finding on information confidentiality had a mean of 1.8, SD 0.1, and overall, the information confidentiality in the six hospitals is good. However, the study found that there are practices that breach information confidentiality such as connecting computers and laptops to more than one network, sharing of electronic devices while transferring electronic data form laptops and desktop

The study revealed that **Information integrity** in the six public Hospitals is poor based on the following i) not all persons authorized to access personally identifiable health data are trained on the organization's information security policies and procedures, the score was slightly above average ii) availability of clearly defined roles to all persons with authorized access to personally identifiable data, not all the hospital have this in place .iii) System to review data accuracy is not available in all the six hospitals assessed. The study finding indicates the following variables to be the worst in terms of promoting information integrity, iv) availability of a designated information security manager at the facility, v) availability of written description of information security manager's responsibilities only, and electronic systems are monitored to detect potential and/or actual security breach, less than half agreed (40%, n= 26) vi) creation of audit logs to track all system transactions in the health facility, slightly more than half agreed on its availability , while half of the respondents agreed that vii) audit logs are reviewed frequently . In regards to risks assessments, the result indicates less than 40% agreed that risk assessments conducted in their facilities, this finding points to a major weakness in the fight against information insecurity and also indication that the information security within the six hospital is at risk. Less than 30% agreed that Risk assessment is conducted Monthly and the same percentage agreed that risk assessment is conducted using the following methods; threat identification, vulnerability assessment, Control analysis, Likelihood determination, impact analysis and Risk determination. information security could be estimated and assessed by doing risk analysis and evaluation. The outcome can assist in planning information security requirements and risk control measures.

**Information availability** According to study findings, availability of information in the six Public hospitals is good based on the following i) updating inventory of computers and mobile devices with personally identifiable health data at (69.9%, n=44) aid in tracking location of computers and monitor for any potential threat to information, ii) The frequency of updating inventories of computers and mobile devices at (61.3% ,n= 38 help identify threats and likelihood of computers being at risk to information damage or loss,iii) updating patient data on desktop and laptop, at (68.2%, n=43) help prevent information loss, duplication, deletion by mistake, virus attack, mixed up even lost. iv) Data Confidentiality and Security Policy shared with patients which scored (36%, n=23) show poor practice since Patients should be informed on the confidentiality and availability of their data to win their trust and v)

audit logs are backed up regularly, at (51%, n=28) this is not good since backing up information is a secure way of maintaining availability of information in case something interferes with the original storage. On average the information availability in the six facilities had (a mean of 2.6, SD 0.1)

From the study findings it can be concluded that the information security frameworks assessed which included (HIPAA, ISO/IEC 27001 and NIPP- RM), did not meet the standards desired for a simple, easy to use and re-adjustable framework that covers the most important components of an information security requirement that follow the right procedure and addresses the most fundamental elements of a framework, it is on this basis this study has proposed and developed an enhanced framework for assessing HIS security Risks .In conclusion .

The study has met its objectives and contributed in terms of assessing the HIS security risks, and also assessing the existing frameworks for assessing HIS security risks giving their strengths and weaknesses which led to development of an enhanced framework for assessing the Health Information Systems security risks which has added knowledge in the field of information security Risks management. The study addresses the literature review gap in line with information security Risks management and operational excellence in higher academic institutions

#### **5.4 Recommendations**

1. Train all persons authorized to access personally identifiable health data on the organization's information security policies and procedures.
2. Providing defined roles to all persons with authorized access to personally identifiable data
3. Putting in place System to review data accuracy.
4. Nominating a designated information security manager in the hospitals,
5. Providing written description of information security manager's responsibilities,
6. creating audit logs to track all system transactions in the hospital,
7. Conducting risks assessments regularly in the Hospitals
9. using enhanced Framework for assessing information security risks in Hospitals
10. Ensuring that information security risks are identified and reduced to manageable level or eliminated completely

### **5.5 Suggestions for Further Studies**

This study was limited to public hospitals, therefore, a similar study can be conducted in private hospitals, Non-Governmental Organization hospitals, and Faith based Hospitals in Kenya to determine whether the findings will be similar. There is also need to conduct further research using more variables besides Confidentiality, integrity and availability of information in Health Sector Further studies are suggested to look at the same topic but using other institutions schools, banks and manufacturing plants to determine the plausibility of these findings. Further, the research used the questionnaire for data collection, with a quantitative methodology. There is need for Other assessments to use other methodology, like a mixed-method (quantitative and qualitative) way of data collection and analysis to test on data triangulation variations

### **6.6 Disclosure of conflict of interest**

The authors hereby declare that they do not have any conflict of any interest.

## REFERENCES

- Abdellatif AA, Al-Marridi AZ, Mohamed A, Erbad A, Chiasserini CF, Refaey Health: toward secure, block chain-enabled healthcare systems. *IEEE Network*. 2020 Apr 22; 34(4):312-9
- Abdulsalam, Y. S., Olaniyi, O. M., & Ahmed, A. (2019). Securing electronic health system using cryptographic technique. *International Journal of Telemedicine and Clinical Practices*, 3(2), 132-155.
- Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. *Journal of big data*. 2018 Dec;5(1):1-8.
- Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV Computing-Assisted Search and Rescue Mission Framework for Disaster and Harsh Environment Mitigation. *Drones*. 2022 Jun 22; 6(7): 1-21.
- Amir Latif RM, Hussain K, Jhanjhi NZ, Nayyar A, Rizwan O. A remix IDE: smart contract-based framework for the healthcare sector by using Block chain technology. *Multimedia tools and applications*. 2020 Nov 10:1-24.
- Amin R, Biswas GP. A secure three-factor user authentication and key agreement protocol for this with user anonymity. *Journal of medical systems*. 2015 Aug; 39(8):1-9.
- Amin R, Islam SH, Gope P, Choo KK, Tapas N. Anonymity preserving and lightweight multimedia server authentication protocol for telecare medical information system. *IEEE journal of biomedical and health informatics*. 2018 Sep 14; 23(4):1749-59.
- Andriole KP. Security of electronic medical information and patient privacy: what you need to know. *Journal of the American College of Radiology*. 2014 Dec 1; 11(12):1212-6.

- Angelis J, Da Silva ER. block chain adoption: A value driver perspective. *Business Horizons*. 2019 May 1; 62(3):307-14.
- Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In *International Conference on Internet of Things as a Service 2022* (pp. 3-18). Springer, Cham.
- Asija R, Nallusamy R. A survey on security and privacy of healthcare data. In *Conference Paper*. July 2014 Jul.
- Ali Z, Hussain S, Rehman RH, Munshi A, Liaqat M, Kumar N, Chaudhry SA. ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments. *IEEE Access*. 2020 Jun 10; 8:107993-8003.
- 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.
- Barman S, Shum HP, Chattopadhyay S, Samanta D. A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme. *IEEE Access*. 2019 Jan 21; 7:12557-74.
- Beck EJ, Gill W, De Lay PR. Protecting the confidentiality and security of personal health information in low-and middle-income countries in the era of SDGs and Big Data. *Global health action*. 2016 Dec 1; 9(1):32089.
- Bendavid Y, Bagheri N, Safkhani M, Rostampour S. Iot device security: Challenging “a lightweight raid mutual authentication protocol based on physical unclonable function”. *Sensors*. 2018 Dec 15; 18(12):4444.
- Bernard R, Bowsher G, Sullivan R. Cyber security and the unexplored threat to global health: a call for global norms. *Global Security: Health, Science and Policy*. 2020 Jan 1; 5(1):134-41.
- Bentotahewa, V., Hewage, C., & Williams, J. (2021). Solutions to big data privacy and security challenges associated with COVID-19 surveillance systems. *Frontiers in big Data*, 4, 645204.
- Burghard C. Big data and analytics key to accountable care success. *IDC health insights*.



2012 Oct; 1:1-9.

Blumberg, B., Cooper, D., & Schindler, P. (2014). EBOOK: Business research methods. McGraw Hill.

Boubaker, S., Houcine, A., Ftiti, Z., & Masri, H. (2018). Does audit quality affect firms' investment efficiency? *Journal of the Operational Research Society*, 69(10), 1688-1699.

Carmines, E. G., & Zeller, R. A. (1979). Reliability and validity assessment. Sage publications.

Chelladurai U, Pandian S. A novel block chain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*. 2022 Jan; 13(1):693-703.

Conaty-Buck S. Cybersecurity and healthcare records. *Am Nurse Today*. 2017; 12(9):62-4.

Chou, T. S., & Chou, T. S. (2011). Information Assurance and Security Technologies for Risk Assessment and Threat Management: Advances. IGI Global.

Chuma KG, Ngoepe M. Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective*. 2022 Mar 4; 31(2):179-95.

Clark, U. Y., & Baltezgar, J. G. (2018). Healthcare information security and assurance.

In *Human-Computer Interaction and Cybersecurity Handbook* (pp. 257-270). CRC Press.

Collen, M.F., Hammond, W.E. (2015). Development of Medical Information Systems (MISs). In: Collen, M., Ball, M. (eds) *The History of Medical Informatics in the United States. Health Informatics*. Springer, London. [https://doi.org/10.1007/978-1-4471-6732-7\\_3](https://doi.org/10.1007/978-1-4471-6732-7_3)

Chander B, Gopala Krishnan K. A secured and lightweight RFID-tag based authentication

protocol with privacy-preserving in Telecare medicine information system. *Computer Communications*. 2022 May 13; 191: 425-437.

Datta, S. P., & Banerjee, P. (2010). Risk management process for information security

- system. *Int J Comput Sci Com*, 1(1), 33-8.
- Disterer, Georg. "ISO/IEC 27000, 27001 and 27002 for Information Security Management." *Journal of Information Security* 04, no. 02 (2013): 92–100. <http://dx.doi.org/10.4236/jis.2013.42011>.
- Dharminder D, Gupta P. Security analysis and application of Chebyshev Chaotic map in the authentication protocols. *International Journal of Computers and Applications*. 2021 Nov 26; 43(10):1095-103.
- Dharminder D, Mishra D, Li X. Construction of RSA-based authentication scheme in authorized access to healthcare services. *Journal of medical systems*. 2020 Jan; 44(1):1-9.
- Farmer Y, Godard B. Public health genomics (PHG): From scientific considerations to ethical integration. *Genomics, Society and Policy*. 2007; 3:14–27.
- Fan K, Jiang W, Li H, Yang Y. Lightweight RFID protocol for medical privacy protection in IoT. *IEEE Transactions on Industrial Informatics*. 2018 Jan 18;14(4):1656-65.
- Farash MS, Nawaz O, Mahmood K, Chaudhry SA, Khan MK. A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. *Journal of medical systems*. 2016 Jul; 40(7):1-7.
- Gope P, Lee J, Quek TQ. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. *IEEE Transactions on Information Forensics and Security*. 2018 May 3; 13(11):2831-43.
- Guo C, Chang CC. Chaotic maps-based password-authenticated key agreement using smart cards. *Communications in Nonlinear Science and Numerical Simulation*. 2013 Jun 1; 18(6):1433-40.
- Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal*. 2018 Jan 1; 16:224-30.
- Grimes, D. A., & Schulz, K. F. (2002). Bias and causal associations in observational

- research. *The lancet*, 359(9302), 248-252.
- Haugen, S., & Rausand, M. (2011). Risk Assessment. In *A Multidisciplinary Introduction to Information Security* (pp. 287-306). Chapman and Hall/CRC.
- Hayale, T. H., & Abu Khadra, H. A. (2006). Evaluation of The Effectiveness of Control Systems in Computerized Accounting Information Systems: An Empirical Research Applied on Jordanian Banking Sector. *Journal of Accounting, Business & Management*, 13.
- Hazard, L. (2016). Is Your Health Data Really Private: The Need to Update HIPAA regulations to Incorporate Third-Party and Non-Covered Entities. *Cath. UJL & Tech*, 25, 447.
- Hao X, Wang J, Yang Q, Yan X, Li P. A chaotic map-based authentication scheme for telecare medicine information systems. *J Med Syst*. 2013 Jun; 37(2): 1–7.
- Houlding D, MSc CI. Health information at risk: successful strategies for healthcare security and privacy. Healthcare IT Program of Intel Corporation, white paper. 2011, 1-8. Xiao, L., Hu, B., Croitoru, M., Lewis, P., & Dasmahapatra, S. (2010). A knowledgeable security model for distributed health information systems. *computers & security*, 29(3), 331-349.
- Hummelholm A. Future Smart Societies' Infrastructures and Services in the Cyber Environments. In *Cyber Security 2022* (pp. 151-182). Springer, Cham.
- Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Artech house.
- ISO/IEC 17799 (2000), In *Information Technology Code of Practice (or information Services*, International Organization for Standardization, Geneva.
- ISACA, & Protiviti. (2020). Today's toughest challenges in IT audit: tech partnerships, talent, transformation. Retrieved 2 March 2020, from [https://www.protiviti.com/sites/default/files/united\\_states/insights/8th-annual-it-audit-benchmarking-survey-isaca\\_protiviti.pdf](https://www.protiviti.com/sites/default/files/united_states/insights/8th-annual-it-audit-benchmarking-survey-isaca_protiviti.pdf).
- Islam SK, Khan MK. Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. *Journal of medical systems*. 2014 Oct; 38(10):1-6.
- Javed AR, Sarwar MU, Beg MO, Asim M, Baker T, Tawfik H. A collaborative healthcare

- framework for shared healthcare plan with ambient intelligence. *Human-centric Computing and Information Sciences*. 2020 Dec; 10(1):1-21.
- Jian G, Feng R. Cryptanalysis and improvement of an improved two factor authentication scheme for telecare medicine information systems. *arXiv preprint arXiv:1607.01471*. 2016 Jul 6.
- Jiang Q, Chen Z, Li B, Shen J, Yang L, Ma J. Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. *Journal of Ambient Intelligence and Humanized Computing*. 2018 Aug; 9(4):1061-73.
- Jiang Q, Ma J, Lu X, Tian Y. Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. *Journal of medical systems*. 2014 Feb; 38(2):1-8.
- Justinia T. block chain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences. *Act Informatics Medica*. 2019 Dec; 27(4):284.
- Kadam, P., & Bhalerao, S. (2010). Sample size calculation. *International journal of Ayurveda research*, 1(1), 55.
- Kavathekar SS, Patil R. Data Sharing and Privacy–Preserving of Medical Records Using Blockchain. In *International Conference on Sustainable Communication Networks and Application 2019 Jul 30* (pp. 65-72). Springer, Cham.
- Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using fuzzy analytic hierarchy process. *Information Systems and e-Business Management*, 15(1), 1-19
- Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81. doi: 10.1080/1097198X.2019.1603527.
- Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. *Journal of medical systems*. 2017 Aug; 41(8):1-9.
- Kui X, Feng J, Zhou X, Du H, Deng X, Zhong P, Ma X. Securing top-k query processing in two-tiered sensor networks. *Connection Science*. 2021 Jan 2; 33(1):62-80.
- Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age

International.

- Kumari S, Renuka K. Design of a password authentication and key agreement scheme to access e-healthcare services. *Wireless Personal Communications*. 2021 Mar; 117(1):27-45.
- Kumar V, Ahmad M, Kumari A. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. *Telematics and Informatics*. 2019 May 1; 38:100-17.
- Liang W, Fan Y, Li KC, Zhang D, Gaudiot JL. Secure data storage and recovery in industrial block chain network environments. *IEEE Transactions on Industrial Informatics*. 2020 Jan 13; 16(10):6543-52.
- Li CT, Lee CC, Weng CY, Chen SJ. A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. *Journal of medical systems*. 2016 Nov; 40(11):1-0.
- Li CT, Shih DH, Wang CC. Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. *Computer methods and programs in biomedicine*. 2018 Apr 1; 157:191-203.
- Liang W, Xie S, Zhang D, Li X, Li KC. A mutual security authentication method for RFID-PUF circuit based on deep learning. *ACM Transactions on Internet Technology (TOIT)*. 2021 Oct 22; 22(2):1-20.
- Liang W, Xiao L, Zhang K, Tang M, He D, Li KC. Data fusion approach for collaborative anomaly intrusion detection in block chain-based systems. *IEEE Internet of Things Journal*. 2021 Jan 22; 1-11.
- Limbasiya T, Sahay SK, Sridharan B. Privacy-preserving mutual authentication and key agreement scheme for multi-server healthcare system. *Information Systems Frontiers*. 2021 Aug; 23(4):835-48.
- Li, S., Bi, F., Chen, W., Miao, X., Liu, J., & Tang, C. (2018). An improved information security risk assessments method for cyber-physical-social computing and networking. *IEEE Access*, 6, 10311-10319.
- Mann, C. J. (2003). Observational research methods. Research design II: cohort, cross sectional, and case-control studies. *Emergency medicine journal*, 20(1), 54-60.
- Marutha N. The application of legislative frameworks for the management

- medical records in Limpopo Province, South Africa. *Information Development*. 2019 Sep; 35(4):551-63.
- Mead CN. Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still difficult. do we really need a better mousetrap? *Journal of Healthcare Information Management*. 2006 Jan 1;20(1):1–21
- Maurya PK, Bagchi S. A secure PUF-based unilateral authentication scheme for RFID system. *Wireless Personal Communications*. 2018 Nov; 103(2):1699-712.
- Ngethe, N. S. (2021). *Information System Security Controls and Data Security in Kiriri Women’s University of Science and Technology, Kenya* (Doctoral dissertation, Kenyatta University).
- Miller, A. R., & Tucker, C. E. (2011). Can health care information technology save babies? *Journal of Political Economy*, 119(2), 289-324.
- Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., de Sousa Junior, R. T., & Nunes, R. R. (2021). Evaluating the performance of NIST’s framework cybersecurity controls through a constructivist multicriteria methodology. *Ieee Access*, 9, 129605-129618.
- Nyakomitta, P. S., Nyangaresi, V. O., & Ogara, S. O. Efficient Authentication Algorithm for Secure Remote Access in Wireless Sensor Networks. *Journal of Computer Science Research*. 2021 Aug; 3(4): 43-50.
- Ngafeeson MN. Healthcare information systems opportunities and challenges. *Encyclopedia of Information Science and Technology*, Third Edition. 2015:3387-3395.
- Nikooghadam M, Amintoosi H. An improved secure authentication and key agreement scheme for healthcare applications. In 2020 25th International Computer Conference, Computer Society of Iran (CSICC) 2020 Jan 1 (pp. 1-7). IEEE.
- Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. *Array*. 2022 Jun 25:100210.
- Nyangaresi VO, Patriotic N. Efficient PUF based authentication protocol for internet of drones. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.
- Otero, A. R. (2019). *Information Technology Control and Audit*. Taylor & Francis group. <https://doi.org/10.1201/9780429465000>.

- Orodho, J. A. (2014). Policies on free primary and secondary education in East Africa: Are Kenya and Tanzania on course to attain Education for All (EFA) Goals by 2015. *International Organization of Scientific Research (IOSR) Journal of Humanities and Social Sciences (IOSR-JHSS)*, 19(1), 11-20.
- Ostad-Sharif, A., Arshad, H., Nikooghadam, M., & Abbasinezhad-Mood, D. (2019). Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. *Future Generation Computer Systems*, 100, 882-892.
- Panigrahi A, Nayak AK, Paul R. HealthCare EHR: A Blockchain-Based Decentralized Application. *International Journal of Information Systems and Supply Chain Management (IJISSCM)*. 2022 Jul 1; 15(3):1-5.
- Pankomera R, van GREUNEN D. Mitigating vulnerabilities and threats for patient-centric healthcare systems in low income developing countries. In *2017 IST-Africa Week Conference (IST-Africa) 2017 May 30* (pp. 1-11). IEEE.
- P Locatelli, N Restifo, L Gastaldi, M Corso - *Innov Informa Syst Modell Tech*, 2012
- Prinsloo, P., & Kaliisa, R. (2022). Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. *British Journal of Educational Technology*, 53(4), 894-913.
- Qiu S, Xu G, Ahmad H, Wang L. A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems. *IEEE access*. 2017 Dec 8; 6:7452-63.
- Radhakrishnan N, Karuppiah M. An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems. *Informatics in Medicine Unlocked*. 2019 Jan 1; 16: 1-38.
- Ravanbakhsh N, Nazari M. An efficient improvement remote user mutual authentication and session key agreement scheme for e-health care systems. *Multimedia Tools and Applications*. 2018 Jan; 77(1):55-88.
- Safkhani M, Vasilakos A. A new secure authentication protocol for telecare medicine information system and smart campus. *IEEE Access*. 2019 Feb 7; 7:23514-26.
- Shamshad S, Ayub MF, Mahmood K, Rana M, Shafiq A, Rodrigues JJ. An identity-based authentication protocol for the telecare medical information system (TMIS) using a physically unclonable function. *IEEE Systems Journal*. 2021 Dec 2: 1-8.

- Shamshad, S., Ayub, M. F., Mahmood, K., Kumari, S., Chaudhry, S. A., & Chen, C. M. (2022). An enhanced scheme for mutual authentication for healthcare services. *Digital Communications and Networks*, 8(2), 150-161.
- Safkhani, M., & Vasilakos, A. (2019). A new secure authentication protocol for telecare medicine information system and smart campus. *IEEE Access*, 7, 23514-23526. (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8460336/>)
- Stoneburner, G., Goguen, A., & Feringa, A. (2002). *A Risk management guide for information technology systems: Recommendations of the national institute of standards & technology*. Retrieved July 6, 2009.
- Silva Rampini, G.H.; Takia, H.; Tobal Berssaneti, F. Critical Success Factors of Risk Management with the Advent of ISO 31000 2018—Descriptive and Content Analyzes. *Procedia Manuf.* 2019, 39, 894–903
- Suresh Kumar V, Amin R, Obaidat MS, Karthikeyan I. An enhanced mutual authentication and key establishment protocol for TMIS using chaotic map. *Journal of Information Security and Applications*. 2020 Aug 1; 53:102539.
- Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of block chain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*. 2019 Jan 2; 3(1):3.
- Song J, Zhong Q, Wang W, Su C, Tan Z, Liu Y. FPDP: flexible privacy-preserving data publishing scheme for smart agriculture. *IEEE Sensors Journal*. 2020 Aug 18; 21(16):17430-8.
- Tewari A, Gupta BB. An internet-of-things-based security scheme for healthcare environment for robust location privacy. *International Journal of Computational Science and Engineering*. 2020; 21(2):298-303.
- Wanyonyi, E., Rodrigues, A., Abeka, S., & Ogara, S. Effectiveness of security controls on electronic health records. *International Journal of Scientific & Technology Research*. 2017 Jan; 6(12): 47–53.
- Wang W, Huang H, Zhang L, Su C. Secure and efficient mutual authentication protocol for smart grid under block chain. *Peer-to-Peer Networking and Applications*. 2021 Sep; 14(5):2681-93.
- Wang X, Fan K, Yang K, Cheng X, Dong Q, Li H, Yang Y. A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living. *Computer Communications*. 2022 Mar 15; 186:121-32.
- Wazid M, Das AK, Kumari S, Li X, Wu F. Design of an efficient and provably secure



- anonymity preserving three - factor user authentication and key agreement scheme for TMIS. *Security and Communication Networks*. 2016 Sep 10; 9(13):1983-2001.
- Weber, G., & Brusilovsky, P. (2001). ELM-ART: An adaptive versatile system for Web-based instruction. *International Journal of Artificial Intelligence in Education (IJAIED)*, 12, 351-384.
- Wright, M. (1999), "Third generation risk management practices", *Computers & Security*, Vol. 1999 No. 2, pp. 9-12.
- Wu F, Xu L, Kumari S, Li X, Das AK, Shen J. A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. *Journal of Ambient Intelligence and Humanized Computing*. 2018 Aug; 9(4):919-30.
- Wood, D. (2019). *Revamping the Privacy Policy: A Study on Informed Consent and User Interactions* (Doctoral dissertation).
- Xu, Zhuo. "An empirical study of patients' privacy concerns for health informatics as a service." *Technological Forecasting and Social Change* 143 (2019): 297-306.
- Xu H, Ding J, Li P, Zhu F, Wang R. A lightweight RFID mutual authentication protocol based on physical unclonable function. *Sensors*. 2018 Mar 2; 18(3):760.
- Xu X, Zhu P, Wen Q, Jin Z, Zhang H, He L. A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. *Journal of medical systems*. 2014 Jan; 38(1):1-7.
- Xiao L, Xie S, Han D, Liang W, Guo J, Chou WK. A lightweight authentication scheme for telecare medical information system. *Connection science*. 2021 Jul 3; 33(3):769-85.
- Yamane T. "Elementary Sampling theory". Englewood Cliffs: Prentice-Hall, Inc (1967).
- Yeboah, T. (2013). A Proposed Information Technology Audit Framework for Microfinance p Kumasi. *Journal of Engineering, Computers & Applied Sciences*, 2(8), 1-7. Retrieved from <https://www.borjournals.com>.
- Zeng X. The impacts of electronic health record implementation on the health care workforce. *North Carolina medical journal*. 2016 Mar 1; 77(2):112-114.
- Zhang, X., Pérez-Stable, E. J., Bourne, P. E., Peprah, E., Duru, O. K., Breen, N., ... &

- Denny, J. (2017). Big data science: opportunities and challenges to address minority health and health disparities in the 21st century. *Ethnicity & disease*, 27(2), 95.
- Zheng L, Song C, Cao N, Li Z, Zhou W, Chen J, Meng L. A new mutual authentication protocol in mobile RFID for smart campus. *IEEE Access*. 2018 Oct 15; 6:60996-1005.  
[https://www.researchgate.net/publication/328310843\\_A\\_New\\_Mutual\\_Authentication\\_Protocol\\_in\\_Mobile\\_RFID\\_for\\_Smart\\_Campus](https://www.researchgate.net/publication/328310843_A_New_Mutual_Authentication_Protocol_in_Mobile_RFID_for_Smart_Campus))
- Zhang L, Zhu S, Tang S. Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. *IEEE Journal of Biomedical and health informatics*. 2016 Jan 12; 21(2):465-75.
- Zhang, Man, Suprateek Sarker, and Jim McCullough. "Measuring information technology capability of export-focused small or medium sized enterprises in China: Scale development and validation." *Journal of Global Information Management (JGIM)* 16.3 (2008): 1-25.
- Zhou Z, Wang P, Li Z. A quadratic residue-based RFID authentication protocol with enhanced security for TMIS. *Journal of ambient intelligence and humanized computing*. 2019 Sep; 10(9):3603-15.

## ANNEXES

### **Annex I: Letter of Transmittal**

**Mathews M. Odiango**

**P.O Box 597 – 40600**

**Siaya**

**14<sup>th</sup> May,2021**

Dear esteemed Respondent,

I am a student at the University of Jaramogi Oginga Odinga Science and Technology, pursuing Master of Science in Health Informatics. I am conducting a research study entitled: An enhanced Framework for Assessing Health Information Systems Security Risks.

You have been selected as a respondent to support in providing data for this research, you are humbly requested to take few minutes and answer the attached questionnaire.

The information you shall provide will be confidential and will be used for academic purposes only. Do not write your name on the questionnaire. You are kindly requested to be honest in your responses.

Thank you for your acceptance to participate.

Yours Faithfully

Henry Mathews Odiango

## **Annex 2: Informed Consent**

### **Consent form**

**Mathews Odiango**  
**P.O Box 597 –40600**  
**SIAYA.**  
**14th, May,2021**

### **Dear Respondent,**

I am a student pursuing Master of Science in Health Informatics University of Jaramogi Oginga Odinga Science and Technology. Currently, conducting a research study entitled: Patient's self-referral decongestion framework for referral hospitals. The finding will be used to support health systems in Kenya and other countries. Hence, countries, communities and individual will benefit from improved quality healthcare services. This research proposal is required to support health systems since it will generate new knowledge in this area that will direct managers in making decisions that are research based. Procedure to be followed in this study respondents will be asked questions and information's will be recorded in the questionnaire. Respondents will not be forced to participate in the study and one will not be victimized or penalized for refusal in participation. In addition, respondent's choice will not be used against him/her nor affect anywhere.

Participation in the study is voluntary. Participants are allowed to ask questions related to the study at any time. Further a respondent will not be forced to respond to questions and he /she can stop any interview at any time without any victimization

### **Discomfort and risks**

Respondents will be asked some personal questions which may make them an ease but

if this happens to an individual, he/she may decide not to respond and may also stop the

interview at any time, the interview may take half an hour to complete

### **Benefits**

Participating in this study will support us in strengthening quality service delivery in Kenya and other countries which have the same problem in study. This research proposal is required to support the health care delivery systems since will create new knowledge in this area thus informing managers in making research based decisions

**Rewards**

**Participants will not be given any reward for taking part in the interview**

Respondents will not be allowed to write their names in that questionnaire to ensure utmost confidentiality is maintained

Contact Information in case of any questions, you may contact the following supervisors;

Professor Silvance Abeka - Lecturer Department of Computer and Software Engineering Jaramogi Oginga Odinga University of Science and Technology Telephone Number: 0710581009

Email: silvancea@gmail.com

Professor Samuel Liyala - Lecturer Department of Computer and Software Engineering

Jaramogi Oginga Odinga University of science and Technology Telephone number: 0718813320 Email: [sliyala@yahoo.com](mailto:sliyala@yahoo.com)

**Participant`s statement**

I have voluntary accepted to take part in the study after being satisfied with the procedure to be followed during the study and being assured that my information will be kept condefintial

Date.....

Signature of interviewee .....

**Investigator`s statement**

I, Confirm, that I have explained to the participant in a language she/he understands the processes to be followed in the study and the risks and the benefits involved.

Name of interviewer.....

Date.....

Interviewer signature.....

**Annex 3: Questionnaire**

This questionnaire is intended to collect research facts concerning an enhanced Framework for assessing Health Information System Security Risks. The questionnaire has two sections. For section A, kindly respond to all items using a tick or type your answer as per the question and for section B, indicate a Yes or No where appropriate. One answer per question. You are requested not to write your name on the questionnaire. I would appreciate your voluntary participation in completing the questionnaire. Thank you.

## SECTION A: RESPONDENT BIODATA

Kindly provide the relevant information by ticking the appropriate box below:

1. Tick the name of the Sub- County

Alego Usonga  Bondo  Gem  Rarieda  Ugenya  Ugunja

2. Write the name of the Hospital .....

3. Write the MFL Code of the Hospital .....

4. Indicate Respondents Gender

Male  Female

5. Indicate respondent age bracket?

20-30Years  30- 40Years

40 -50Years  50-60Years

60 Years and above

6. What is your professional Training background?

Medical doctor  Nurse  Environmental Health Science officer

Nutritionist  Pharmacist  Health Records and information officer

Clinical officer  Physiotherapist  Other Specify.....

7. What is your Level of professional Training?

Primary  Secondary

Certificate  Diploma

Bachelor Degree  Master Degree

PhD

8. Where are you stationed in this hospital? .....

9. Do you use computer in performing your duties?

Agree  Disagree  don't know  Not Applicable

10. If yes in Question 9, what do you use the computer for? (select all that apply) If no go to QZ number 11

Data Entry  Report writing  Data Analysis  Entertainment  sending reports

**SECTION B: ASSESSING HIS INFORMATION SECURITY RISKS**

**Table 2: information confidentiality**

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>strongly disagree</b>	<b>Disagree</b>	<b>mean</b>	<b>std Deviation</b>
staff need a user identifier and password to gain access to a computer							
computers permitted to be connected to more than one network							
policies state that staff is personally responsible for protecting paper records, computer workstations, laptop computers associated with confidential information							
written policy available for ensuring the confidentiality, security and privacy of personally identifiable health data							
The facility is using emails, flash discs, intranet, external hard disk, file transfer protocol, optical media and smart card in transferring electronic data							

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>strongly disagree</b>	<b>Disagree</b>	<b>mean</b>	<b>std Deviation</b>
within a site,							
The facility is using access privileges, encryption Antivirus security to protect information during transmission (in %)							
Facility is using Physical measures for protecting patient privacy while collecting information							
Physical security control's in place to prevent unauthorized access to buildings and rooms containing personally identifiable health data,							
<b>Average</b>							

Source (Author ,2020)



**Table 3: Information Integrity**

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>Strongly Disagree</b>	<b>disagree</b>	<b>Mean</b>	<b>Std Deviation</b>
all persons authorized to access personally identifiable health data trained on the organization's information security policies and procedures							
Are there clearly defined roles to all persons with authorized access to personally identifiable data?							
a designated information security manager available at the facility							
a written description of the information security manager's responsibilities available							
system to review data a curacy in this facility available							
Availability of documented processes for							

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>Strongly Disagree</b>	<b>disagree</b>	<b>Mean</b>	<b>Std Deviation</b>
handling data inaccuracies							
electronic systems are monitoring to detect potential or actual security breach							
audit logs are created to assist in recording all system transactions							
Data is reviewed frequently for accuracy							
Audit logs are reviewed frequently							
Monitoring of electronic systems to detect potential or actual security breaches doe regularly							
electronic systems are monitored regularly							

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>Strongly Disagree</b>	<b>disagree</b>	<b>Mean</b>	<b>Std Deviation</b>
Are risk assessments conducted in your facility							
risk assessment is conducted monthly							
The following Methods are used to conduct risk assessment Threat identification, vulnerability assessment, Control analysis, Likelihood determination, impact analysis and Risk determination?							
Does the facility use intrusion Detection systems							
Is there reward and sanctions for going against the policies							
Does the Facility have incident							

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>Strongly Disagree</b>	<b>disagree</b>	<b>Mean</b>	<b>Std Deviation</b>
reporting mechanism in place							
Does the Facility have proper devices disposal mechanism							
Facility has devise isolation mechanism							
Is there emergency contingency protocols in place in this facility							
<b>Average</b>							

Source (Author ,2020)

**Table 4: Information Availability**

<b>Statement</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>Strongly Disagree</b>	<b>disagree</b>	<b>Mean</b>	<b>Sdt Deviation</b>
Facility has updated inventory of computers and mobile devices containing personally identifiable health data							

Inventory of computers and mobile devices records are updated regularly							
patient data on desktop and laptop are updated frequently							
Data Confidentiality and Security Policy shared with patients							
Facility audit logs are backed up regularly							
data on desk top and laptop are backed up, regularly							
Audit logs are backed up regularly							
<b>Average</b>							

Source (Author ,2020)

### Annex 4: Work plan

**Table 10: Research Work Plan**

Months	2018	2019			2020				2021 and 2022				2023	
	Sept-Dec	Jan-Mar	April -June	July -Dec	Jan -March	Apr -June	July -Sept	Oct -Dec	Jan-Mar	Apr-June	July-Sept	Oct-Dec	Jan-Mar	Apr--July
Developing Proposal Document														
Literature Review														
Proposal / Defense at Departmental level														
Defense at (Faculty Level)														
Proposal Presentation														
Pre Testing														
Data Collection														
Data Analysis														
Report Writing														
Mock Presentation														
Mock Corrections														
Thesis Presentation														
Thesis consultation with supervisors														
Oral Presentation Corrections														
Final Submission of Thesis														

**Annex 5: Research Budget**

**Table 11: Research Budget**

<b>ITEM</b>	<b>UNIT</b>	<b>PRICE PER UNIT</b>	<b>TOTAL</b>
Writing pads	1 ream	400/=	400/=
Pens	6	30/=	180/=
Pencils	5	30/=	150/=
Erasers	4	40/=	80/=
Sharpeners	3	20/=	60/=
Printing papers	3 reams	500/=	1500/=
Stapler	1	500/=	500/=
Stapler pins	3 packets	60/=	180/=
Paper punch	1	500/=	500/=
Box file	2	500/=	500/=
Internet services	3 hrs/day/50	50/= per hour	3600/=
Typing and printing	80 pages	10/=	800/=
Airtime	60 days	60/= per day	3600/=
Transport to consult supervisors	5 trips	1000/=per trip	5000/=
Proposal binding	4copies	500/= per copy	2000/=
Questionnaires printing	50 copies	30/=per copy	1500/=
Data collection	30 days	500/=per day	15000/=
Data analysis	5days * 1 pax	1000 per day	5000/=
Final dissertation binding	6 copies	600/= per copy	3600/=
10% Contingency			4,766.50
<b>GRAND TOTAL</b>			<b>52,431.60/=</b>

## ANNEX 6: JOUST ETHICAL RESEARCH POLICY (ERC) APPROVAL



**JARAMOGI OGINGA ODINGA  
UNIVERSITY OF SCIENCE AND TECHNOLOGY  
DIVISION OF RESEARCH, INNOVATION AND OUTREACH  
JOUST-ETHICS REVIEW OFFICE**

Tel: 057-2501804  
Email: [erc@joust.ac.ke](mailto:erc@joust.ac.ke)  
Website: [www.joust.ac.ke](http://www.joust.ac.ke)

P.O. BOX 210 - 40601  
BONDO

OUR REF: JOUST/DVC-IU/ERC/12

7<sup>th</sup> June, 2021

Henry M. Ondiogo  
1153/4224/2017  
JOUST

Dear Mr. Ondiogo,

**RE: APPROVAL TO CONDUCT RESEARCH TITLED "A FRAMEWORK FOR ASSESSING HEALTH INFORMATION SYSTEMS SECURITY AND PRIVACY RISKS"**

This is to inform you that JOUST ERC has reviewed and approved your above research proposal. Your application approval number is ERC7/6/21-26. The approval period is from 7<sup>th</sup> June, 2021 – 6<sup>th</sup> June, 2022. 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 JOUST IERC.
- 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 NACOSTI IERC within 72 hours of notification.
- iv. Any changes, anticipated or otherwise that may increase the risks of affected safety or welfare of study participants and others or affect the integrity of the research must be reported to NACOSTI IERC 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 JOUST IERC.

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

Yours sincerely,


A handwritten signature in black ink, appearing to read 'Francis Ang'wa', is written over a circular stamp or seal.


Prof. Francis Ang'wa  
Chairman, JOUST ERC

Copy to: Deputy Vice-Chancellor, RIO    Director, BPS    Dean, SIS




**ANNEX 7: NACOSTI APPROVAL**

  
REPUBLIC OF KENYA

  
NATIONAL COMMISSION FOR  
SCIENCE, TECHNOLOGY & INNOVATION

Ref No: 194481 Date of Issue: 16 July 2021


**RESEARCH LICENSE**




This is to Certify that Mr. Henry Mathews Odongo of Jaramogi Odinga Odongo University of Science and Technology, has been licensed to conduct research in Slaya on the topic: **A FRAMEWORK FOR ASSESSING HEALTH INFORMATION SYSTEMS SECURITY AND PRIVACY RISKS** for the period ending : 16 July 2022.

License No: NACOSTI/P/21/11562

194481  
Applicant Identification Number

  
Director General  
NATIONAL COMMISSION FOR  
SCIENCE, TECHNOLOGY &  
INNOVATION

Verification QR Code



NOTE: This is a computer generated License. To verify the authenticity of this document,  
Scan the QR Code using QR scanner application.

## ANNEX 8: COUNTY DIRECTOR OF HEALTH APPROVAL

### COUNTY GOVERNMENT OF SIAYA



### DEPARTMENT OF HEALTH AND SANITATION

E-mail: [siayachd@gmail.com](mailto:siayachd@gmail.com)  
ADIACENT TO ICC CHURCH  
PHONE:  
SIAYA TOWN

COUNTY HEALTH HEADQUARTERS  
SIAYA COUNTY  
P O BOX 597  
SIAYA

Our Ref: CGS/CHD/RESEARCH/VOL/IV (105)

30<sup>TH</sup> JUNE, 2021

- All Medical Superintends  
Siaya County

#### RE: CLEARANCE TO CONDUCT A STUDY ON FRAMEWORK FOR ASSESSING HEALTH INFORMATION SYSTEMS SECURITY AND PRIVACY RISKS

Henry Mathews Odango is a student of Jaramogi Oginga Odinga University of Science and Technology pursuing his Master of Science in Health Informatics.

He has received authorization from National Commission for Science, Technology & Innovation (NACOSTI) - JOOUST Ethics Review Committee (vide Ref: JOOUST/DVC-RIO/ERC/E2) to conduct the above referenced study in our county.

The study sites will be the 10 Hospitals in the County.

#### Specific Objectives:

1. To examine existing Health Information System security and privacy risk.
2. To assess available frameworks for assessing security of HIS.
3. To develop integrated framework for assessing security of HIS.

This is to notify you that the Research has been approved by the office of the undersigned

Kindly accord him the necessary support.

Thank you.

  
Dr. Felix Tindi  
County Pharmacist  
County Government of Siaya



#### Copy to:

- ✓ CECM – Health and Sanitation
- ✓ Ag. Chief Officer – Health and Sanitation