CHALLENGES ENCOUNTERED IN USING INFORMATION SECURITY METRICS TO IMPROVE PATIENT SAFETY IN PUBLIC HOSPITALS, NAIROBI METROPOLITAN, KENYA

MARYANNE WAITHERA MWAURA

S201/CTY/PT/37461/2017

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF LAW, ARTS AND SOCIAL SCIENCES IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTERS IN SECURITY MANAGEMENT AND POLICE STUDIES, KENYATTA UNIVERSITY

NOVEMBER, 2025

DECLARATION

This project is my original work and has not been presented for a degree in any other university.

Signature _____ Date _____

Maryanne Waithera Mwaura

S201/CTY/PT/37461/2017

This project has been submitted with my approval as the university supervisor:

Signature _____Date _____

Dr. Bernard Munyao Muiya

Department of Security, Diplomacy and Peace Studies

Kenyatta University

ACKNOWLEDGMENT

I am profoundly thankful to my family for their prayers and material assistance toward the realization of my goal of completing this research project. I extend my sincere appreciation to my supervisor, Dr Muiya, for his guidance, patience, and insightful feedback throughout this journey. I also wish to thank the Kenyatta University staff at the School of law, arts and social sciences for their mentorship and supportive academic environment. Above everything else, I am grateful to God Almighty for His sustenance and the wisdom He has graciously bestowed upon me for the successful conclusion of this research project.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

AI	Artificial Intelligence
AIC	Africa Inland Church
AMREF	African Medical and Research Foundation
APHIA Plus	AIDS, Population and Health Integrated Assistance Plus
CDC	Centers for Disease Control and Prevention
CDS	Clinical Decision Support
CDSS	Clinical Decision Support Systems
CHIS	Community Health Information Systems
CINAHL	Cumulative Index to Nursing and Allied Health Literature
COVID	Coronavirus Disease
CPOE	Computerized Provider Order Entry
CTY	City
DHIS	District Health Information System Software
EFA	Exploratory Factor Analysis
EHR	Electronic Health Records
EMR	Electronic Medical Records
ERC	Ethics Review Committee
FHI	Family Health International
GKPS	Global Knowledge Sharing Platform for Patient safety
GOK	Government of Kenya

HIM	Health Information Metrics
HIS	Health Information Systems
HIT	Health Information Technology
HMIS	Health Management Information System
HMN	Health Metrics Network
HSOPS	Hospital Survey on Patient Safety Culture
ICT	Information and Communication Technology
IHRIS	Integrated Human Resource Information System
IOM	Institute of Medicine
ISM	Information Security Metrics
ISSA	Information Systems Security Association
ISSM	Information Systems Success Model
KEMSA	Kenya Medical Supplies Authority
KMTC	Kenya Medical Training College
KNBS	Kenya National Bureau of Statistics
KNH	Kenyatta National Hospital
KUERC	Kenyatta University Ethics Review Committee
KUTRRH	Kenyatta University Teaching, Referral & Research Hospital
LMIS	Logistic Management Information System
MER	Medical Error Reporting
MOH	Ministry of Health

MPSC	Multi-Professional Patient Safety Curriculum
NGO	Non-Governmental Organizations
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
QSR	Qualitative Software Research
SDG	Sustainable Development Goals
SPSS	Statistical Package for Social Sciences
STS	Socio-Technical Systems
TAM	Technology Acceptance Model
TIBA	M-TIBA (Mobile Health Wallet)
UN	United Nations
UON	University of Nairobi
USAID	United States Agency for International Development
WHO	World Health Organization

OPERATIONAL DEFINITION OF TERMS

Health care interventions: Acts performed on behalf of an individual or population whose aim is to evaluate, upgrade and sustain health.

Patient safety: Prevention of errors and harm that occur to patients during provision of health care.

Information Security: Prevention of unauthorized access, alteration and disclosure of information.

Metrics: Tools of measuring, comparing and tracking performance or production in an organization to facilitate decision making.

Security Metrics: Instruments designed to boost accountability and enable decision making through reporting, acquisition and evaluation of security data.

Healthcare workers: People in a hospital that provide medical care to individuals or community.

Electronic Health Record: Software enabled electronic format of a patient's clinical record and treatment history.

Safety risks: Possibility of harm while in a healthcare organization.

Report: A written or spoken account of an event that one has observed to a specific audience and purpose.

Patient flow: Movement of patients, information between departments and among hospitals as part of patient care.

ABSTRACT

Ideally, majority of people who visit a healthcare facility do so with the purpose of getting medical treatment. The person goes in with the confidence that medical treatment is accurate and safe, so they have the best chance possible of achieving the desired outcome. The sad reality is that correct and safe medical treatment is not always achieved. Patient information is one of the resources that hospitals heavily rely on to achieve its goals. This study investigated the challenges of using Information Security Metrics in public referral hospitals in Nairobi Metropolitan, Kenya. The specific objectives were to; examine the technical components of Information Security Metrics and their effects on promoting patient safety, determine security controls that protect the Privacy, Integrity and Accessibility of data in Information Security Metrics in promoting patient safety, ascertain key patient safety reporting systems in Information Security Metrics that help in reducing medical errors and analyse the legal challenges of using Information Security Metrics to promote patient safety with reference to the Kenyan Data Protection Act, No. 24 of 2019. Socio-Technical Systems Theory guided the study. The study adopted a cross-sectional survey design. Data was collected using questionnaires and interview guide. Two hundred and eighty-eight respondents from healthcare workers, ICT staff and health records personnel were sampled through cluster, simple random and purposive sampling methods. Quantitative data analysis was done using SPSS through illustrative, correlation and Principal Component Analysis, while thematic analysis was used for qualitative data. The findings revealed that technical components such as data collection software and backup generators promoted patient safety, but challenges included inadequate staff training. Security controls like firewalls and antivirus software were critical, though procedural weaknesses, such as inconsistent password management, limited their impact. Patient safety reporting systems lacked well-developed infrastructure, with 50.9% disagreeing that adequate systems were in place, while mandatory reporting of ISM issues was key to improving reporting culture. Moreover, legal frameworks prioritized patient privacy and confidentiality, though patient engagement remained moderate. The study demonstrated that while technical, procedural, and legal elements of ISM contribute significantly to patient safety, gaps in implementation and engagement persist. The study thus concludes that effective implementation of Information Security Metrics (ISM) is necessary for improving patient safety in healthcare facilities. In view of the findings, the study recommends improvement of infrastructure, enforcement of procedural consistency, and strengthening patient engagement to maximize the effectiveness of ISM in healthcare facilities. Also, the hospitals should consider prioritizing the development and implementation of comprehensive training programs for staff on the use of ISM tools and protocols.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The chapter provides a background that outlines how Information Security Metrics is applied to improve patient safety. The section presents how patient records were stored before the emergence of technology. Healthcare sector has embraced the use of technology and consequently the application of Information Security Metrics to enhance patient safety, but not without challenges. This forms the foundation of the principal focus of the research: to study the challenges of using Information Security Metrics to improve patient safety. The subsequent segments of the chapter highlight the research questions, importance of the research study, the scope and delimitations.

1.2 Background of the Study

Health care interventions are designed to benefit people, but unfortunately, they sometimes are hazardous to the patient. Data collected from different parts of the world indicate that at least 10% of patients are harmed while receiving health care in developed countries (WHO, 2017). Multiple stakeholders from WHO have created a network known as the Global Knowledge Sharing Platform for Patient safety (GKPS), the network raised the issue that health care systems still lack a timely and systematic means of dispensing information on patient safety incidences. To address this gap, GKPS applied the use of Information Security Metrics so as to learn from reported incidences (WHO, 2017). Information Security Metrics provides insights to identify strengths and weaknesses in an organization. Patient information stored in Electronic Health Records is very important and sensitive to both the patients and the physicians. It is essential for health care providers to have updated and correct information on the patient to reduce cases of medical errors. Thus, the confidentiality, availability and integrity

of all patient information must be fully protected when using Information Security Metrics. When there is a breach of the three security aspects patient safety ends up being compromised. Health care personnel awareness on ISM helps transform raw data into actionable information that will reduce cases of medical errors. The information gathered facilitates proper resource allocation, planning of safer operation procedures, and disaster and recovery planning (Warkentin, Mcbride, Carter, & Johnston, 2016).

Traditionally, patient reports were recorded on paper, stored in folders and only one copy was obtainable. Technology has laid the foundation for Electronic Health Records which has made patient information easy to read and available from almost every location in the world. It has not only changed the format of patient records, but it has also improved patient safety. Such transitions have led to increased development and adoption of Information Security Metrics to improve its impacts on patient safety (Alotaibi & Federico, 2017).

The principal objective of these projects was to revolutionize the collection, presentation, dissemination and preservation of patient data with the intention of refining patient safety, while the auxiliary aim was to design upgrades for their health care delivery systems (Vuokko, Vakkuri, & Palojoki, 2022). However, all these projects have experienced significant obstacles that often lead to substantial disruptions in the usual health care processes (Palojoki, Saranto, Reponen, Skants, Vakkuri, & Vuokko, 2021). Electronic Health Records contains a lot of patient information, most of which is considered protected health information. The advancement of technology has seen an increase in cyber threats which hinders privacy and security of patient information, any alteration of this information by unauthorized personnel can lead to medical errors. ISM is tasked with collecting timely data that enables hospital management to make accurate, timely and informed decision based on evidence presented.

Safety risks identification by health care facilities using Information Security Metrics to identify areas in patient safety that need improving (Alotaibi & Federico, 2017). Ensuring that

relevant hospital staff acquires sufficient training on Information Security Metrics (Waddell, 2024). For instance, Clinical officers point out that they are under staffed, adding the task of data collection on them has them feeling over worked, when faced with the challenge of recording data or saving a life, they opt to save lives first since that is the main task assigned to them (Alotaibi & Federico, 2017). Managing electronic health information presents unique challenges; a response to these challenges is using Information Security Metrics. Data gathered from the ISM help to make evidence based decisions in order to improve patient safety. Encouraging the practice of data collection among health care providers ensures that the culture of using ISM is developed to improve patient safety.

Health care management deals with sensitive information and it is the obligation of policy makers to facilitate Information Security Metrics education and on regular basis training (Larsen, Fong, Wernz, & Ratwani, 2018). The role of ISM in health systems is more than the routine collection of data, it facilitates evidence based decision making on patient safety. Inadequate skills in ISM, the perception of ineffectiveness of data gathered at collection levels usually creates a low level of commitment from health workers. Lack of Information Security Metrics awareness itself is a potential security threat to sensitive information and overall may result in patient harm. The absence or poor support from the management of institutions may lead to under reporting of patient safety incidences. Additionally, it could lead to a culture of rudimentary information generation and utilization, leading to flawed mechanisms for validating and assuring patient safety (Jenkins, Sharfeen, Moinudheen, Pathan, & Thomas, 2020).

In addition, these countries face the challenges of ransomware attacks, unauthorized access, and data leaks which jeopardizes patient confidentiality and interferes with hospital operations, delaying critical care (Ahouanmenou, Van Looy & Poels, 2023). Moreover, there is issue with inconsistent data governance and interoperability, where hospitals use different EHR systems

that do not effectively communicate with each other, leading to fragmented patient records and potential medical errors (Alsahli, et al., 2024). Additionally, insufficient staff training and awareness further complicate information security, as healthcare providers often lack the necessary cybersecurity knowledge, making them vulnerable to phishing attacks and accidental data mishandling (Neri, et al., 2024). Research done by Makary and Daniel (2016) indicates that clinical blunders are ranked third as reasons for mortality in the USA.

On the global stage, Australian, Canadian, United Kingdom, Belgium, Denmark and the United States of America (USA) governments have invested billions of dollars in Health Information Metrics, including Electronic Health Records (EHRs), for the long term (Charlotte, Marion, George, & Joan, 2016). However, despite these investments, hospitals in these countries continue to face serious challenges in using information security metrics to improve patient safety. One such challenges is data breaches and cybersecurity threats, as healthcare systems remain prime targets for cybercriminals due to the sensitive nature of patient data (World Health Organization, 2023).

Regionally, the healthcare sector in South Africa has experienced an increase in security threats and breaches, with the industry incurring the highest per capita data breach costs among various sectors in 2019 (Chuma, 2019). This increase in cyber incidents compromises patient confidentiality and undermines trust in digital health systems. In Nigeria, the rapid adoption of digital health systems has outpaced the implementation of adequate cybersecurity measures, leaving healthcare organizations exposed to data breaches and cyberattacks (Andersen Nigeria, 2023). This vulnerability is compounded by insufficient training for healthcare workers on cybersecurity best practices, leading to inadvertent data mishandling and exposure. Rwanda's healthcare system, while advancing in digital health initiatives, still grapples with limited resources and infrastructure to support effective information security frameworks, making it challenging to implement security metrics effectively. Similarly, Uganda faces hurdles due to

the heterogeneity of health information systems, which lack standardized data structures and exchange protocols (Bagyendera, Nabende, Godman, & Nabukenya, 2024). This inconsistency hinders the establishment of unified security metrics and complicates the monitoring and protection of patient data across different platforms.

In Kenya, the United Nations (UN) launched the Sustainable Development Goals (SDG) in September 2015 putting the spotlight on the need for better data to track the progress and inform decision making on patient safety. However, according to MOH in Kenya, timely and relevant data that helps decision makers are in short supply (MOH, 2020). Inadequate data often leads to making decisions that are not based on evidence, therefore not helping to improve patient safety cases. Several investments have been developed to boost health care quality. One such venture is the upgrading of health information systems across the spectrum of data collection, information development, analysis and application, to support productive decision-making among producers and consumers of health care information (WHO, 2018). Despite the investments made in Information Security Metrics, health care facilities still experience challenges in improving quality of patient safety. MOH (2020) describes such challenges as an enormous data array at different levels often stored in varying formats across diverse systems and locations, making access, distribution and evaluation difficult.

The culture of using Information Security Metrics is not fully adopted in the Kenyan health care field due to the weak legislative system that coordinates and manages health related information development across different actors and sectors (Ajwang', Komen, & Ngaira, 2019). For ISM to function optimally, it has to be fully embraced by all relevant hospital staff. Hospitals should have a strong legal framework that ensures; consent is given during collection of data, data is stored safely in order to maintain data confidentiality and integrity. Currently, there are multiple similar data acquisition systems where data for the health care sector is stored in various databases like the District Health Information System Software (DHIS-2), Kenya

National Bureau of Statistics (KNBS), Electronic Health Records (EHRs) etc. (MOH, 2018). The availability of multiple data collection systems that are not interconnected could create a situation where there is numerous data duplication and time wastage during data acquisition and management. Ajwang', Komen and Ngaira (2019) also states that Kenya has received massive attention on Health Information Metrics and despite the attention received; the country still lacks productive and effective Health Information Metrics. It therefore undermines evidence-based decision making process which could lead to an increase in medical errors. The Berwick review indicates that currently, majority of the health care organizations have limited capacity to evaluate, track or capitalize on safety and quality information (Berwick, 2013, p. 27). The review cited that the gap as costly and should be closed. It is against this background that the research shall be conducted to find out what challenges are faced by public hospitals in Nairobi Metropolitan in using Information Security Metrics with the goal of improving patient safety.

Kenya began growing its Information Security Metrics in 1976 through an experimental project aided by the United States Agency for International Development (USAID) (MOH, 2018). Over recent decades, the Government of Kenya (GOK) has formulated tactical plans and frameworks to fortify cooperation coordination between private firms and nongovernmental organizations (NGOs), availed specific guidelines on HIS, incorporated data acquisition and presentation tools, enhanced data flow and advanced feedback mechanisms (Alotaibi & Federico, 2017).

In 2013, Kenya decentralized its power from the national to the county level. The national MOH is now in charge of helping counties in formulating their own HIS strategic programs and guidelines (MOH, 2020). The counties are responsible for drafting and implementing HIS legislation, framework and guidelines; creating Electronic Medical Record (EMR) systems; allotting funds; growing human resources; and fusing health program information systems in a

central HIS. External stakeholders include AIDS, Population and Health Integrated Assistance Plus (APHIA Plus), African Medical and Research Foundation (AMREF), Centers for Disease Control and Prevention (CDC) and WHO. These parties offer technical support and mechanisms to promote a harmonized HIS, by expanding Information distribution and encouraging data use for decision making (Sabi, Uzoka, Langmia, Njeh, & Tsuma, 2018). The data is a precious asset (Kean & Cochrane, 2021) that helps make the best possible decisions (Liu, 2022).

The Kenya HIS has various data feeds that are incorporated with DHIS-2, the national platform for the administration of everyday health data. Sub counties, social health workers and health centers submit data that are amassed at the county and national levels to DHIS-2 (MOH, An assessment of patient safety standards in Kenya, 2020).

Some other data feeds connected to DHIS-2 are the CHIS (Community Health Information Systems), the iHRIS (Integrated Human Resource Information System) and the LMIS (Logistic Management Information System). Community Health Information Systems) supplies data from communities and health centers through social health workers. IntraHealth developed iHRIS; it presents data on personnel management, including the number and groups of health personnel and providers. The Kenya Medical Supplies Authority (KEMSA) with technical assistance from management Sciences for Health and FHI 360, manages LMIS, which is responsible for commodity requests from counties and healthcare institutions (MOH, 2020). DHIS-2 was configured to carry out quality data analysis, monitor and evaluate health care programs. It has facilitated personalized data evaluation, which has promoted utilization of data for making decisions right from the lowermost level (Pitt, Dryzek, & Ober, 2020).

1.3 Statement of the Problem

Ideally, majority of people who visit a healthcare facility do so with the purpose of getting medical treatment. The person goes in with the confidence that medical treatment is accurate and safe so they have the best chance possible of achieving the desired outcome. The sad reality is that correct and safe medical treatment is not always achieved. Patient information is one of the resources that hospitals heavily rely on to achieve its goals. If patient information is compromised, patient safety is likely to suffer serious consequences in the form of patients having the wrong limb amputated, administering incorrect dosage of medicine and in some other instances the patient ends up dying.

A retrospective analysis at Kenyatta National Hospital (KNH) from 2019 to 2021 revealed that 40% of the 640 reported medical errors were diagnostic in nature, often leading to delayed or incorrect treatments (Okutoyi et al., 2024). Despite the implementation of Medical Error Reporting (MER) systems, underreporting remains a critical issue; only 38.1% of healthcare workers at KNH who encountered errors formally reported them, primarily due to fear of punishment and inadequate feedback mechanisms (Okutoyi et al., 2022). Furthermore, a nationwide assessment of 493 health facilities indicated that over 90% scored below acceptable patient safety standards, with leadership and accountability processes scoring particularly low (World Bank Group, 2022). These deficiencies are compounded by insufficient information security measures; a study assessing data protection in Nairobi's health facilities found that many lacked proper strategies to safeguard patient data, increasing the risk of errors stemming from compromised information (Ayugi, 2021).

Research findings like the ones by Makary and Daniel (2016) have led to development of over half a dozen data collection agencies in Kenya. Despite such measures by the Kenyan government, the use of Information Security Metrics to improve patient safety is still facing challenges because cases of medical errors are still being reported. Despite recommendations

given by Kenya Patient Safety survey report on how Information Security Metrics can be applied to enhance patient safety, cases of medical errors are still being reported. Thus, it is essential to establish why ISM is not improving patient safety by asking fundamental questions: is it because of insufficient training and awareness on ISM or ineffective security controls or inadequate patient safety reporting systems? Therefore, the researcher sought to identify the challenges experienced by public hospitals in Nairobi Metropolitan in using Information Security Metrics to promote patient safety.

1.4 Research Objectives

The general objective of the study was to investigate the challenges associated with the use of Information Security Metrics to improve patient safety at public referral hospitals in Nairobi Metropolitan. The specific objectives were to:

1. Examine the technical components of Information Security Metrics and their effects on promoting patient safety.
2. Determine security controls that protect the Privacy, Integrity and Accessibility of data in Information Security Metrics in promoting patient safety.
3. Ascertain key patient safety reporting systems in Information Security Metrics that help in reducing medical errors.
4. Analyse the legal limitations of using Information Security Metrics to promote patient safety with reference to the Kenyan Data Protection Act, No. 24 of 2019.

1.5 Research Questions

There was need to understand how technical components, security controls, reporting systems and legal challenges affect the use of Information Security Metrics to improve patient safety. From this premise, the study therefore asked the following questions:

1. Which security controls safeguard the Privacy, Integrity and Accessibility of data in Information Security Metrics?
2. What security measures are employed on ISM hardware and software?
3. What reporting systems are used in Information Security Metrics to promote patient safety?
4. What are the legal limitations of using Information Security Metrics?
5. Who receives training and awareness on Information Security Metrics?
6. What is the combined effect of technical ISM components, security controls, patient safety reporting systems, and legal frameworks on promoting patient safety?

1.6 Justification and Significance of the Study

The aim of this study was to determine the challenges encountered by health care facilities while using Information Security Metrics to improve patient safety. The findings of this study may increase awareness to all stake holders in the healthcare sector and to the hospital management of the challenges encountered in the use of Information Security Metrics towards improving patient safety and enable them to formulate appropriate strategies, guidelines and standards to safeguard patient's information and avoid cases on medical error.

The policy makers may use the findings to form a background for development of strong Information Security Metric strategies, guidelines and standards in Hospitals which can be implemented towards improving the safety of the patient. The research may be significant to researchers since this study may supplement the existing knowledge on Information Security

Metrics and shall provide reference material to scholars. The research findings may form a basis for further studies on how Information Security Metrics may improve patient safety.

1.7 Scope of the Study

The research project was performed to reveal the drawbacks in using Information Security Metrics to improve patient safety in government hospitals in Nairobi Metropolitan. The aspects that were looked at included ISM technical components, the hospital security culture in reporting of ISM related incidences, the response rate to the reported incidents and the security controls present that maintain the confidentiality, availability and integrity of patient data.

1.8 Limitations and Delimitations of the Study

The study encountered several limitations that affected its scope and execution. First, the research was conducted within the Nairobi Metropolitan area, specifically focusing on public referral hospitals, which limited the generalizability of the findings to private hospitals and public healthcare facilities. This geographic restriction may have excluded unique challenges faced by hospitals in other regions of Kenya, especially those with different levels of technological developments and resource allocation. Additionally, the study achieved a response rate of only 41.9% of the distributed questionnaires. This limitation was primarily attributed to the busy schedules of healthcare professionals, reluctance to disclose security-related challenges due to fear of repercussions, and institutional restrictions on sharing sensitive data. Furthermore, access to key hospitals such as Kenyatta University Teaching, Referral & Research Hospital (KUTRRH) was denied, reducing the sample size and potentially limiting the comprehensiveness of the study. The study also faced financial constraints, which restricted the researcher's ability to expand data collection efforts and conduct extensive field visits to verify certain claims made in the responses.

Despite these limitations, the study had key delimitations that ensured a focused and manageable research scope. The research deliberately concentrated on public referral hospitals due to their significant role in patient care and high volume of patient records, making them ideal for studying the challenges of Information Security Metrics (ISM) in improving patient safety. The choice of Nairobi Metropolitan was based on its high concentration of public referral hospitals, availability of digital health infrastructure, and the presence of relevant stakeholders in health data management. The study was also delimited to assessing specific technical components of ISM, security controls, patient safety reporting systems, and legal challenges, ensuring a structured and in-depth analysis of key areas affecting information security in hospitals. The use of both questionnaires and interview guides helped in gathering diverse opinions from healthcare workers, ICT officers, and health records personnel, mitigating the risks of data insufficiency. Additionally, ethical considerations were strictly adhered to, with approvals obtained from Kenyatta University Ethics Review Committee (KUERC) and the National Commission for Science, Technology, and Innovation (NACOSTI), ensuring compliance with research regulations and ethical standards. By focusing on Nairobi Metropolitan's public hospitals, the study provided valuable insights that can be used as a benchmark for improving ISM practices in similar healthcare settings.

.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The chapter reviews literature applicable to this research by exploring the technical components of using Information Security Metrics, the security controls, reporting procedures and legal challenges of using ISM from a global, regional and local perspective. It also looks at the theoretical and conceptual framework.

2.2 Empirical Review

Information Security is described as the prohibition of and restoration from, unsanctioned or unwanted corruption, alteration, distribution or utilization of information and information facilities whether intentional or unintentional (Michael, Nicolas, & Philipp, 2021). Security metrics are instruments devised to assist in the decision-making process and to boost operation and transparency through collection, evaluation and publication of data (Dilli, Simon, Jin-Hee, Terrence, & Nelson, 2020). Since the 1990s significant contributions in data acquisition have enhanced the knowledge and understanding of global health, but vast gaps remain between what health practitioners know and what they need to know to ameliorate patient safety (Astier, Carlet, & Hoppe-Tichy, 2020).

O'Brien, Ghafur, & Durkin (2021) explains patient security as the lack of evitable injury to a patient amid the healthcare process and the decrease of unwarranted damage connected to

medical services to the least possible minimum. O'Brien, Ghafur, & Durkin (2021) also states that, patient safety issues rarely receive attention in developing countries, resulting in scarcity of information regarding patient safety. The scenario that there is scarcity of information regarding patient safety indicates a gap that if not addressed are likely to lead to an increase in medical errors. The lack of attention has been linked to health system constraints, including human resource shortages and difficulty in obtaining reliable data (Wambugu & Villella, 2020).

Information Security Metrics has been enforced in various health institutions in Malaysia, Japan, South Korea and Australia with the main benefits being improving patient safety quality by boosting the timeliness and precision of records and management information. Katuu (2016) confirms that Information Security Metrics provides a solid platform for improving patient safety. For instance, the application of ISM in hospitals helps the healthcare givers to have accurate patient records that assists to make informed decisions and reduce medical errors.

In 2007, Sierra Leone was chosen among Health Metrics Network's (HMN) experimental countries for the improvement of health information systems. Its success is ascribed to the participation of different stakeholders in data collection and complimented by training on the use and analysis of data (Marlee & Devi, 2019). In 2005, with endorsement from the Danish International Development Agency, the Health Management Information System (HMIS) in Zanzibar's MOH, launched a program designed to boost data reporting, collection and implementation (Tim & Kari, 2019). Such studies are clear proof that ISM training, stakeholder involvement and strengthening data reporting can improve patient safety.

The potential for Electronic Health Records to upgrade the standards, security and effectiveness of healthcare delivery has been acknowledged since the 1960s (Linda, Hannah, Allison, & Heather, 2017). EHRs have been a vital cornerstone, because of their ability to abate errors through distribution of applications like Computerized Provider Order Entry (CPOE) and

Clinical Decision Support (CDS) and reduction of errors that can cause adverse medical problems (Benet, 2017). ISM particularly CDS and CPOE improves health process adherence, medication orders, lab orders and improved patient safety. ISM is made up of hardware and software which are prone to theft and malware attack. Thus, the adoption of EHRs presents the risk of hardware and software malfunction where data can be lost or corrupted during distribution (Klaus, Susanne, & Martyn, 2019). Healthcare management with funding from hospital stakeholders can apply physical security controls on the ISM hardware and ensure updated software and fire walls to prevent system failures and access by unauthorized users. During the processing of any information among stakeholders of healthcare providers, Information Security Metrics should adopt properties of CIA (Andres, 2014). Adoption of CIA properties advocates for; not sharing patient records without permission, ensuring that patient data is reliable, consistent and accurate and lastly making patient information available to the healthcare givers at the right place and time. This ensures that information cannot be accessed by unauthorized users (Cabric, 2015). This property ensures that only those with access have permission to alter the information. Organizations should provide on demand reliable, consistent and accurate data on patient information (Cabric, 2015). The information should be present at the right time and place to the authorized users (Andres, 2014).

2.2.1 Technical Components of Information Security Metrics and Patient Safety

Adeyemi, Adegoke, and Odugbose (2024) explored the impact of healthcare information technology (HIT) on reducing medication errors by reviewing advancements in electronic health records (EHRs), clinical decision support systems (CDSS), barcoding technology, telemedicine, and mobile health applications. Using a systematic literature review, the study synthesized evidence from scholarly sources and real-world implementations. The findings indicated that HIT significantly minimized medication errors by automating prescription processes, enhancing clinical decision-making, and improving communication among

healthcare providers. However, challenges such as system interoperability issues, financial constraints, cybersecurity risks, and resistance to technology adoption hindered full implementation. The study concluded that HIT enhances patient safety but requires strategic investments, improved interoperability, and enhanced cybersecurity measures. The study addressed a key gap by specifically evaluating HIT's role in medication error reduction and highlighting disparities in HIT adoption between developed and resource-constrained healthcare systems.

A study by Olusanya and Peter (2024) analyzed the impact of digitalization on the healthcare industry in Nigeria, focusing on clinics as the primary access points for medical services. The study employed a mixed-methods approach, using both interviews and questionnaires to gather data. Findings indicated that while the digitalization of Nigerian clinics is long overdue, its implementation is influenced by technological, organizational, user-related, economic, and social factors. Among these, organizational factors had the most significant impact, while economic and social factors were the least influential. The study concluded that digitalization is critical for improving healthcare services in Nigeria and provided a framework for its implementation. This research presented a contextual gap by focusing on clinics in Nigeria rather than public referral hospitals in Nairobi Metropolitan, where challenges in using Information Security Metrics (ISM) to enhance patient safety remain underexplored. It also filled a conceptual gap by examining digitalization broadly rather than specifically investigating ISM and its role in reducing medical errors, which remains a key challenge in Nairobi’s public healthcare facilities.

Mujuni et al. (2024) examined how a locally developed diagnostic connectivity solution in Uganda facilitated the real-time collection and transmission of high-quality data on infectious diseases to the national health dashboard between May 2022 and May 2023. The study successfully configured a digital health technology on 260 sites, integrating diagnostic

instruments such as GeneXpert, Truenat, and digital X-ray devices to provide over 927,000 test results for disease surveillance and patient care. The findings revealed that sustained internet connectivity, stakeholder engagement, strong laboratory coordination, and integration with existing health data tools were critical for the successful implementation of the system. However, poor bandwidth in some locations was a significant barrier to effective connectivity. The study concluded that diagnostic connectivity solutions play a vital role in strengthening healthcare data collection and disease control efforts. Conceptually, the study focused on real-time diagnostic data connectivity for disease surveillance rather than investigating Information Security Metrics (ISM) and their role in patient safety, leaving a gap in understanding how ISM impacts error reduction in hospital settings. Contextually, the study was conducted in Uganda and focused on diagnostic laboratories, whereas the current study addressed these gaps by investigating the challenges associated with the use of ISM in improving patient safety in public referral hospitals within Nairobi Metropolitan, where medical errors and data security challenges remain pressing concerns.

According to a study by Zare, Olsen, Zare, & Azadi (2018), patient safety related data can be applied in multiple functions, such as selection of improvement programs, evaluation of success of patient safety improvement efforts, enhanced accountability through public reporting and organization accreditation. Reporting relies on the user-friendliness of a reporting system, the corporate's security culture and attitude towards disclosure of errors. For instance, nurses with diverse patient care requirements might lack time to report despite his/her belief in the significance of reporting. Fear of retribution or litigation could lead to under reporting. Healthcare organizations should learn from their mistakes. Thus, identified mistakes are educational opportunities that encourage intervention to prevent potential risks to patients. Correct decisions rely on sound data. Therefore, it is crucial that data be readily available to its users and of good quality. A strong Health Information System (HIS) is the bedrock of a robust

medical care structure and efficient HIS avails accurate information to the correct people at the appropriate time, ensuring legislators and service providers make informed decisions on patient care.

According to WHO (2020), Patient safety can be affected if the information on the patient is incomplete or inconsistent and poor quality data can lead to incorrect decisions that can be unfavorable to patient safety. Therefore, clumsy and disintegrated data acquisition systems are unreliable and ineffective in providing data required for decision making (AlHogail, 2015). In relation to ensuring Information Security Metrics, technological methods (such as fire walls and passwords) that safeguard information may be effective. However, most data losses are not due to inadequate or defective technology, but result from technology users and wrong human behavior; thus, encouraging ISM training and awareness courses among healthcare givers could go a long way in improving patient safety (Chang & Ramachandran, 2015). Technical safety measures are effective, but should be accurately stated, designed, enforced, framed and sustained to perform optimally and reduce cases of medical errors in hospitals (Burisch & Wohlgemuth, 2016).

2.2.2 Security Controls that Protect Privacy, Integrity and Accessibility of Data and Patient Safety

Bani Issa et al. (2020) explored privacy, confidentiality, security, and patient safety concerns associated with the use of electronic health records (EHRs) among nurses in the United Arab Emirates. Using a mixed-method approach, the study collected data from 562 nurses between January and June 2018 through surveys and focus group discussions. The findings revealed that 48% of nurses were concerned about EHR security, particularly administrative-related security risks, inadequate training, and unauthorized access. Additionally, patient safety concerns were largely attributed to non-technological factors, such as lack of audit mechanisms, poor communication with technology vendors, and excessive time required for

documentation. Focus group discussions further highlighted inconsistencies in data integrity policies as an issue. Conceptually, the study focused on nurses' concerns about EHR security and patient safety but did not investigate the specific role of Information Security Metrics (ISM) in improving patient safety, leaving a gap in understanding how ISM frameworks address security threats in hospital settings. Methodologically, the study relied on self-reported concerns rather than an empirical evaluation of ISM implementation and its impact on reducing medical errors. The current study addressed these gaps by investigating the challenges associated with using ISM to enhance patient safety in public referral hospitals in Nairobi Metropolitan.

Jawad (2024) examined security and privacy challenges in digital healthcare systems, highlighting risks associated with the digitization of medical records, including data breaches, unauthorized access, ransomware attacks, and potential misuse of patient data. The study explored the implications of widespread digital adoption in healthcare and emphasized the need for robust security measures to protect patient privacy and maintain data integrity. The research presented key mitigation strategies, such as strong encryption protocols, multi-factor authentication, secure communication channels, and cybersecurity training for healthcare professionals. However, the study focused on the broader security and privacy challenges in digital healthcare but did not specifically examine the role of Information Security Metrics (ISM) in mitigating security threats within hospital settings. Contextually, the research was global in scope, lacking a specific focus on public referral hospitals in Nairobi Metropolitan, where medical errors and systemic information security challenges persist. The current study addressed these gaps by investigating the challenges associated with using ISM to enhance patient safety, particularly in Nairobi's public hospitals.

A study by Hamapa et al. (2024) explored healthcare workers' and patients' perceptions and experiences regarding biometric technology in Zambian healthcare settings, focusing on its

implementation challenges and benefits. The phenomenological study was conducted in four healthcare facilities in Lusaka Province, where biometric technology was actively used. Data were collected through face-to-face interviews with 20 healthcare workers and 16 patients, as well as focus group discussions, with transcripts analyzed using Nvivo version 12 and inductive thematic analysis. The findings revealed that facilitators of biometric adoption included efficient system integration, investment in biometric equipment, workflow transformation, and improved patient recognition. However, barriers included infrastructure limitations, technical challenges, patient resistance, misconceptions, and accessibility issues for individuals with disabilities. The study concluded that biometric systems have the potential to enhance healthcare efficiency and data integrity, but their success depends on education, improved infrastructure, and addressing cultural resistance. Since the study focused on biometric identification in healthcare access and data integrity, it presented conceptual gap since it did not explore the role of Information Security Metrics (ISM) in patient safety, leaving a gap in how ISM frameworks can reduce security risks and medical errors. Methodologically, the study used qualitative phenomenological analysis without assessing the quantitative impact of ISM on patient safety outcomes. The current study addressed these gaps by investigating challenges in using ISM to improve patient safety in public referral hospitals in Nairobi Metropolitan, where medical errors and information security concerns remain a critical issue in healthcare service delivery using quantitative and qualitative data.

Findings of a study by Faozi, Najib, Ali, Borhan and Mohd (2022) indicated that senior officials' support topped the list of twenty-five security challenges affecting Information Security Metrics. The study indicated that Information Security Metrics should not only be focused on end-users and on technical features but should have an administrative focus as it is a management issue. The cost of implementing Information Security Metrics to incorporate all kinds of hardware and software is very high (Menard, Bott, & Crossler, 2017). Therefore,

management should set aside funds that may cater for updating and upgrading of hardware and software in the hospital relating to ISM in order to improve patient safety. According to Omar (2017), authentic and timely health information is a vital component for public health action especially when resources are scarce, and financial backing can be the distinction between life and death.

In Kenya, Kimathi (2024) examined the impact of cloud computing on data security in healthcare, using M-TIBA, a cloud-based platform for managing healthcare finances and data, as a case study. Grounded in the Technology Acceptance Model (TAM) and the Information Systems Success Model (ISSM), the study employed a mixed-methods approach, integrating quantitative surveys and qualitative interviews. Data were collected from M-TIBA users, healthcare providers, and IT policymakers, with a sample of 450 participants, yielding 360 usable responses. Quantitative data were analyzed using statistical correlations, while qualitative data provided insights into trust and technology adoption. The findings indicated that higher digital literacy improved adoption and trust in cloud security, but limited user awareness remained a barrier. While M-TIBA users expressed moderate satisfaction with security measures, concerns over data breaches and unauthorized access were significant among healthcare providers, emphasizing the need for better transparency in data protection practices. The study concluded that user education is critical for cloud security effectiveness and recommended routine digital literacy programs, improved security protocols, and greater transparency in data handling. Conceptually, the study focused on cloud computing and data security in financial and health data management but did not address Information Security Metrics (ISM) in improving patient safety. Contextually, the study focused on M-TIBA users and financial health data rather than public referral hospitals in Nairobi Metropolitan. The current study addressed these gaps by investigating the challenges in using ISM to enhance patient safety in Nairobi's public hospitals.

2.2.3 Key Patient Safety Reporting Systems in Information Security Metrics and Medical Errors

Ferrara et al. (2024) conducted a systematic review to examine the role of artificial intelligence (AI) in clinical risk management and patient safety. The study aimed to investigate how AI enhances risk prevention, incident identification, and reporting in healthcare settings. Using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, a systematic review of 297 articles was conducted across SCOPUS and Medline (via PubMed) databases, ultimately selecting 36 relevant studies. The findings identified three primary "incident type" domains where AI contributes to patient safety: clinical process management, healthcare-associated infections, and medication errors. Additionally, AI was found to improve incident reporting systems, aiding healthcare providers in identifying and analyzing adverse events more efficiently. The study concluded that while AI significantly enhances clinical risk management and patient safety, it requires human supervision and cannot fully replace healthcare professionals' decision-making. Conceptually, the study focused on AI-driven clinical risk management rather than the role of Information Security Metrics (ISM) in preventing medical errors and ensuring patient safety, leaving a gap in understanding how ISM contributes to reducing risks. Methodologically, the study systematically reviewed existing literature but did not conduct empirical field research to assess ISM effectiveness in real-world hospital settings. The current study addressed these gaps by investigating the challenges in using ISM to enhance patient safety in Nairobi’s public hospitals using cross-sectional data.

A study by Janusz, Steven, William and Andrew (2018) revealed that insufficient Information Security Metrics awareness initiatives point to a serious shortcoming in efficient Information Security Metrics enforcement. The study indicated that to increase the application of medical data in developing countries, it is necessary to improve medical personnel’s feeling of data

ownership and eradicate the assumption that the medical workers' responsibility ceases when they obtain data and convey it to the subsequent level. The most common causes of data security issues are human error, hackers, privacy policy violation and software errors. The study also pointed out that due to the increased use of Information Security Metrics, many health care institutions have formed Information Security Metrics awareness programs to ascertain that their employees know the various securities of risks, thereby protecting the safety of the patient.

In a separate study, Mensah et al. (2024) investigated ethical, security, and patient safety concerns associated with Digital Health Technologies (DHTs) among healthcare professionals in Ghana. The study employed a mixed-methods research design, incorporating a descriptive survey and in-depth interviews with healthcare professionals across three tertiary hospitals between July and September 2022. Thematic content analysis was conducted using QSR NVivo 12, while Stata 15 was used for quantitative analysis, generating percentages, means, and standard deviations. A total of 369 health professionals participated in the study, with 81.03% expressing concern over patient health data disclosure without consent, making it the most frequently cited issue. The study concluded that health professionals were highly concerned about patient information security and emphasized the importance of strict access control policies, periodic updates of safety protocols, and better enforcement of cybersecurity measures to prevent human errors from compromising security systems. Methodologically, the research relied on self-reported data from healthcare professionals, lacking an empirical evaluation of ISM effectiveness in hospitals. The current study addressed these gaps by investigating ISM challenges in public referral hospitals in Nairobi Metropolitan, where data security issues and patient safety risks remain critical concerns in healthcare service delivery.

In their study, Nthumba, Mwangi, and Odhiambo (2024) examined patient safety culture in a rural sub-Saharan African hospital, focusing on AIC Kijabe Hospital in Kenya over a seven-

year period. The study used the Hospital Survey on Patient Safety Culture (HSOPS) tool to assess, build, and sustain institutional safety culture. The HSOPS tool, without local modifications, was distributed to all 650 hospital employees during surveys conducted in 2013, 2015, 2017, and 2019. The average response rate over the study period was 84.5% (range: 65.1% to 93.6%). Findings showed significant improvements in patient safety culture, with positive dimension scores increasing in 2019 and hospital support for patient safety improving significantly). Additionally, staff turnover decreased, and the overall patient safety grade (excellent/very good) reached 50%. The study highlighted institutional leadership challenges, high staff turnover, and evolving hospital leadership structures as key obstacles in developing and maintaining a robust patient safety culture. However, it concluded that patient safety can be successfully improved in sub-Saharan Africa through dedicated safety champions and strong institutional leadership. The study focused on building a safety culture using HSOPS but did not examine the role of Information Security Metrics (ISM) in preventing medical errors and enhancing patient safety, hence conceptual gap. The current study addressed the gap by investigating ISM challenges in public referral hospitals in Nairobi Metropolitan.

2.2.4 Legal Challenges of Using Information Security Metrics to Promote Patient Safety

Reddy (2025) examined the global harmonization of Artificial Intelligence-Enabled Software as a Medical Device (AI-SaMD) regulation, focusing on the challenges and the need for unified standards. Given the lack of cohesion in regulatory frameworks, the study reviewed key regulations from the United States, the European Union, China, and Australia, identifying divergences in approaches to algorithm transparency, risk management, data security, and clinical evaluation. The findings emphasized the need for globally harmonized AI-SaMD regulations, advocating for international standards and global data security protocols to enhance AI-driven medical device safety and effectiveness. Additionally, cross-border cooperation was recommended to establish consistent security and risk management practices.

The study however focused on AI-enabled medical device regulation but did not explore the role of Information Security Metrics (ISM) in ensuring patient safety within hospital settings, leaving a gap in understanding how ISM frameworks contribute to mitigating security threats in healthcare environments. Methodologically, the study was policy-oriented and regulatory-focused, lacking empirical evaluation of ISM implementation in real-world healthcare institutions. The current study addressed these gaps by investigating ISM challenges in public referral hospitals in Nairobi Metropolitan, where security vulnerabilities in health information systems directly impact patient safety and clinical risk management.

Elsewhere, Solimini et al. (2021) examined the ethical and legal challenges of telemedicine during the COVID-19 pandemic, highlighting unresolved regulatory concerns in the rapidly expanding field of telehealth services. The study conducted a narrative review using a literature search on PubMed, analyzing 85 articles published between March 2019 and September 2021, of which 24 were deemed eligible for review. The findings revealed that key ethical and legal concerns included informed consent and patient autonomy (87%), data protection and security (74%), patient privacy (78%) and confidentiality (57%), malpractice and professional liability (70%), and equity of access and quality of care (30%). The study emphasized that standardized regulations are needed to ensure equitable healthcare access, data security, and patient confidentiality while preventing legal ambiguities surrounding professional liability and malpractice. The study concluded that telemedicine should only serve as a complementary or supplementary tool alongside traditional healthcare services until comprehensive ethical and legal frameworks are established. Methodologically, the study conducted a narrative review, rather than an empirical investigation of security vulnerabilities in hospital-based digital health systems. Contextually, the research examined telemedicine globally, whereas the current study addressed these gaps by investigating ISM challenges in public referral hospitals in Nairobi

Metropolitan, where data security threats and patient safety risks remain critical concerns in digital healthcare adoption.

McGivern, Wafula, Seruwagi, Kiefer, Musiega, Nakidde and English (2024) examined health professional regulation in Kenya and Uganda, focusing on how weak enforcement impacts professional practice and patient care in low- and middle-income countries (LMICs). The study employed large-scale research conducted between 2019 and 2021, incorporating 29 national regulatory stakeholders, 47 subnational regulatory actors, doctors, and nurses, alongside a national survey of 3,466 doctors and nurses. Data were analyzed using thematic analysis, exploratory factor analysis, and focus group discussions to validate findings. The study found that regulatory bodies in Kenya and Uganda were perceived as resource-constrained, remote, and ineffective in preventing malpractice and ensuring adequate professional education and training. However, participants viewed online licensing and regulation positively, particularly where regulators-maintained relationships with healthcare professionals. Based on these findings, the study proposed an "ambidextrous" approach to improving regulation, referred to as deconcentrating regulation, which involves enhancing online licensing, streamlining regulatory administration, and using freed resources to develop localized regulatory offices and strengthen professional oversight. Conceptually, the study focused on regulatory frameworks and their impact on healthcare practice but did not address how Information Security Metrics (ISM) could enhance regulatory oversight and mitigate security-related risks in hospital settings, leaving a gap in understanding ISM's role in improving patient safety. The current study addressed these gaps by investigating ISM challenges in public referral hospitals in Nairobi Metropolitan, where weak regulatory enforcement, digital security vulnerabilities, and patient safety concerns are critical issues in healthcare service delivery.

Dissanayake, Dharmasena, and Warnakulasuriya (2024) examined the challenges of integrating patient safety (PS) concepts into nursing curricula, focusing on the barriers to

implementing the World Health Organization's Multi-Professional Patient Safety Curriculum (WHO-MPSC) introduced in 2011. While some developed countries have established their own PS frameworks, many nations have yet to fully integrate these concepts into pre-licensure healthcare education. To synthesize the challenges hindering the integration of PS into nursing education, the study conducted an integrative literature review covering 2011–2022, searching CINAHL, MEDLINE, and Google Scholar using keywords related to barriers, challenges, nursing students, and PS education. Twenty reviews met the inclusion criteria, leading to the identification of five challenge categories: educators' characteristics, administration, program structure, curriculum content, and the theory–practice gap. In total, 17 specific challenges were identified, including insufficient faculty training in PS concepts, lack of institutional support, rigid curricula, and gaps between theoretical instruction and clinical application. Conceptually, the study focused on nursing curricula and education challenges but did not examine the role of Information Security Metrics (ISM) in improving patient safety in hospital settings, leaving a gap in understanding how ISM can prevent medical errors and enhance healthcare security. The current study addressed the gap by investigating the challenges of using ISM to enhance patient safety in Nairobi's public hospitals.

2.3 Theoretical Framework

This study was anchored on Socio-Technical Systems (STS) theory. Socio-Technical Systems theory was originally formulated in 1960 by experts Eric Trist and Fred Emery, in Tavistock Institute in London (Martin, Ali, Steve, & Paulo, 2018). Savaget and Acero (2017) argue that enterprises should be approached as social technical structures where social and technical networks are merged to maximize their productivity. When social and technical structures are analyzed in the framework of ISM in the health sector, the correspondences are evidence-based decision making, improved patient safety and increased productivity. This means that when

hospital staff are encouraged and taught to embrace the use of ISM decision making is evidence based to improve the safety of the patients.

The theory states that corporate structures consist of behavioral and technical structures that are both self-sufficient and interactive (Abbas, Pitt, & Michael, 2021). This is applicable in the health sector considering that hospital staffs (social systems) are tasked with saving lives while ISM is tasked with using different technologies (technical systems) to collect accurate data in order to make informed decisions. Both components are independent faculties but to achieve patient safety they both have to be interactive. Social system portion of the theory explores the individuals in an organization and their interactions within the organization's structure (Bednar & Welch, 2020). This component is useful to the study because it clearly shows how healthcare staff interact among themselves and with the patients within a hospital.

The technological element of the theory handles the operations and tasks inside the company and the technology required to run the systems in the organization (Emery, 2016). The STS theory demonstrates the various ISM technical components that manage data collection, management and analysis in a healthcare facility in order to make informed decision based on data provided. STS theory is crucial for organizations due to the proportionate increase of technology in organizational processes. Consequently, businesses tend to cooperatively maximize their enterprises' social and technological proportions, and they should pay attention to the interconnection of the constituents for improved application of the utilities (Kapoor, Ziaee, Dwivedi, Schroeder, Beltagui, & Baines, 2021). STS theory is used in various spheres of organizational development, such as Information Security Metrics design.

The implementation of STS theory in Information Security Metrics is observed in a study by Noel (2016). The study describes Information Security Metrics of a firm, including formulating and maintaining algorithms, in relation to STS theory frames and constituents. The researchers contend that Information Security Metrics is frequently seen from a more technical perspective

(Noel, 2016). However, it is crucial to note that health care facilities should also consider hospital staff perspectives and involvement along with technical ease of use and efficiency. Healthcare facilities should consolidate both technological and social aspects of the ISM to improve patient safety.

The Socio-Technical Systems (STS) theory was considered relevant and applicable to the current study because it was important in explaining the challenges associated with the use of Information Security Metrics (ISM) to improve patient safety at public referral hospitals in Nairobi Metropolitan. This theory provided a framework for analyzing the interaction between healthcare workers, security systems, data management policies, and the overall hospital environment. The technical component involved the use of ISM tools such as encryption, access controls, network monitoring, and data audits to secure patient records and minimize medical errors. However, technology alone is insufficient without addressing the social aspect, which includes healthcare personnel's digital literacy, adherence to security protocols, resistance to technology adoption, and ethical concerns surrounding data access and sharing. Moreover, the STS framework was essential in examining how the misalignment between security technologies and human behavior contributed to data breaches, compromised patient safety, and operational inefficiencies. Through the application of STS theory, the study was able to identify the socio-technical challenges hindering effective ISM implementation, such as lack of cybersecurity training among medical personnel, fragmented IT governance, and inadequate hospital investments in security infrastructure. STS theory was instrumental in exploring the systemic barriers affecting ISM efficiency in Nairobi Metropolitan public hospitals and in proposing balanced solutions that bridge technological innovation with human adaptability, ultimately enhancing patient safety and data security in healthcare environments.

2.4 Conceptual Framework

The researcher applied the causal effect correlation between independent and dependent variables as shown in Figure 2.1 to conduct the study on challenges faced by ISM in improving patient safety at public hospitals in Nairobi Metropolitan. To improve patient safety (dependent variable) in the hospital, the researcher has identified independent variables in Information Security Metrics as ISM technical components, security controls, reporting systems and the legal challenges. The intervening variable shall be the hospital security culture.

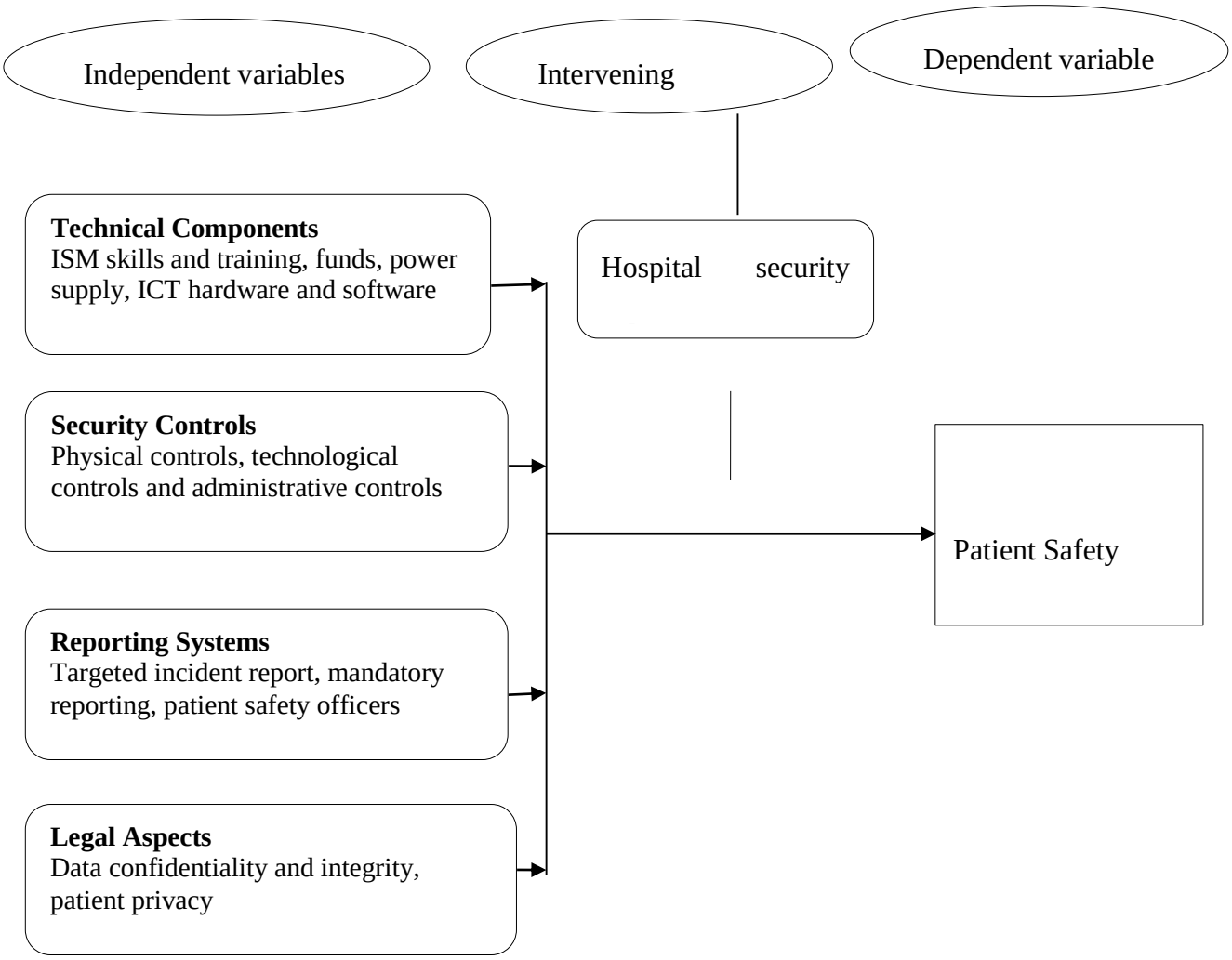


Figure 2.1: Conceptual Framework

Source: Derived from literature review

The researcher sought to identify the technical components of ISM (independent variable) and its effects on patient safety (dependent variable). The researcher also identified the current hospital reporting systems (independent variable) and rate of response to reported cases effect on patient safety (dependent variable). The researcher found out the legal challenges of using ISM (independent variable) and how they affect patient safety (dependent variable). Since patient information was very sensitive, the researcher identified the security controls

(independent variable) established to safeguard the confidentiality, availability and integrity of patient details and how it affects patient safety (dependent variable).

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the methodology employed to investigate the challenges associated with Information Security Metrics in enhancing patient safety. It details the research design, criteria for selecting hospitals, and provides an overview of the target population. The chapter also presents the sampling procedures and the rationale behind determining the sample size. Furthermore, it delves into the tools and methods used for data collection, alongside the procedures followed for testing validity and reliability. A pilot study is included to refine the approach before full implementation. Additionally, the chapter covers the data management and analysis techniques, ensuring the integrity of the findings. Ethical considerations are also thoroughly examined to guarantee that the research is conducted with the highest standards of professional and moral responsibility.

3.2 Research Design

The study gathered data from hospitals in Nairobi metropolitan through a cross-sectional survey. The researcher gathered data needed to evaluate challenges encountered when using ISM and its effects on patient safety in four public hospitals. The researcher adopted the design because enabled data collection from a cross section of respondents at a specified time (Ponto, 2015). Therefore, data was gathered data from government hospitals in Nairobi Metropolitan in a short span of time. Another benefit of employing cross-sectional research design was that it enabled the examination of a population with diverse traits, which enabled the researcher to record multiple findings and derive correlation (Julia, 2018). The design was useful because it was fast, easy and economical to perform, particularly for the interviews.

3.3 Site Selection and Description

As the capital city of Kenya, Nairobi County is also the largest city in the country. The data obtained from the 2019 census indicates that Nairobi has the largest population of 4, 397,073. Out of the five public referral hospitals in Kenya, Nairobi Metropolitan has four, thus the highest number of public referral hospitals in Kenya. Therefore, this study was carried out in Public Referral Hospitals in Nairobi Metropolitan because of the large numbers of patients and patient records received. The four referral hospitals are namely: Kenyatta National Hospital, Mathari National Teaching and Referral Hospital, National Spinal Injury Referral Hospital and Kenyatta University Teaching Referral and Research Hospital. Kenyatta National Hospital is the oldest hospital in Kenya with a capacity of over 1,800 beds. It is a teaching and referral hospital and also the second largest hospital in East Africa. The hospital is located in Upper Hill; Hospital Road, Nairobi. Mathari National Teaching and Referral Hospital is the largest teaching and referral psychiatric hospital in Kenya with a bed capacity of over 600. It is located in Nairobi, Muthaiga along Thika Highway. National Spinal Injury Referral Hospital is a national level six hospital with a capacity of over 30 beds. It is located in Nairobi, Kilimani; Lenana Road. It specializes in the treatment of spinal cord injuries. Kenyatta University Teaching Referral and Research Hospital is a modern Public National referral hospital with a bed capacity of over 650. It is located in Kahawa West, Nairobi Northern Bypass.

The study thus targeted the four referral hospitals in Nairobi Metropolitan, namely Kenyatta National Hospital, Spinal Injury Referral Hospital, Mathari National Teaching and Referral Hospital and Kenyatta University Teaching Referral and Research Hospital (KUTRRH). However, permission was not granted to collect data at KUTRRH with the hospital management citing cessation of data collection at the hospital. The large patient flow from the targeted hospitals assisted to find out most of the challenges faced in using Information Security Metrics to improve patient safety.

With decision-making of patient safety being highly dependent on information, most of the public referral hospitals have embraced the use of Information Security Metrics but cases of medical errors are still being reported. This study therefore was undertaken in Nairobi Metropolitan because it has the largest number of referral hospitals using Information Security Metrics.

3.4 Target Population

The intended population for the research compromised healthcare workers, ICT officers and health records personnel. Healthcare workers were drawn from health care departments. The healthcare workers targeted included medical officers, nurses, clinical officers, and laboratory technologists, as they are the primary users of Information Security Metrics (ISM) in patient care. The target population was selected among the three sub-sectors because they are the respondents that mainly interact with ISM therefore, they easily pointed out the challenges experienced in using ISM and how the challenges affect patient safety.

3.5 Sampling Procedures and Sample Size

This segment illustrates techniques that were used to obtain the sampling size for the research and the study respondents selected.

3.5.1 Sample Size Determination

The researcher used precision and confidence level criteria to calculate the size of the sample. To attain this, the researcher repeatedly gathered data from the populace and work out the mean. The mean figure acquired from the sample was the representative of the actual population value (Ponto, 2015). The precision level was a marginal error of plus or minus 5% and confidence level used was 95%. The workings are as shown below:

$$n = p(1-p)\left(\frac{Z}{E}\right)^2$$

Where n = the sample size

Z is the appropriate z value for desired confidence level

E is the desired margin of error

p = is the sample proportion

q = 1-p.

The confidence level = 95 per cent, thus, the z value = 1.96

The margin of error was 0.05.

In this case,

$$n = 0.5(1 - 0.5)\left(\frac{Z}{E}\right)^2$$

$$n = 0.5(1 - 0.5)\left(\frac{1.96}{0.05}\right)^2$$

$$n = 384.2$$

To make sure the 95% confidence interval estimate of the portion of healthcare personnel is within 5% of the actual population, a sample of 384 was used. The sample was fairly distributed to the three sub-sections resulting to 128 per sub section. This was then divided equally among the three study sites, giving 32 respondents per site. However, permission was not granted to collect data at KUTRRH with the management citing cessation of data collection in the hospital Since approval to collect data at KUTRRH was not granted due to a cessation of research activities, data collection proceeded only in the remaining three hospitals Kenyatta National Hospital, Spinal Injury Referral Hospital, and Mathari National Teaching and Referral Hospital. Each of these hospitals therefore contributed 32 respondents per sub-section, giving

96 respondents per sub-section across the three hospitals, and a total of 288 respondents for all three sub-sections combined (96 × 3 = 288).

3.5.2 Sampling Technique

This study applied simple random sampling, cluster, and purposive sampling techniques. Purposive sampling was employed to choose respondents from; ICT officers and health records personnel. The researcher believes that they were the key participants who provided ample and accurate data on the challenges in using ISM to improve patient safety. The researcher used the hospitals as boundaries and created clusters for every one of the four study sites. Multi stage cluster was applied to sample healthcare workers. The healthcare departments formed the clusters from which samples were collected.

At the first point, the researcher listed the healthcare workers from the healthcare departments with the help of the head of departments. Stage two was involved choosing of groups from which the sample was obtained. Simple random sampling was utilized. The final stage involved proportionate selection of the total number of respondents from the healthcare workers in each cluster that was sampled. Individual healthcare workers were identified using simple random sampling. Healthcare workers in the chosen clusters were given numbers. A random number generating application was used to select the sample.

3.6 Data Collection Procedures

This project used questionnaires and interview guide as the project tools.

3.6.1 Questionnaires

Questionnaires was the basic tool of data acquisition for the research. The questionnaire sampled the targeted sample respondents. It was administered face-to-face to evaluate the level of comprehension and knowledge the participants had information security metrics. The items

were measured using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

3.6.2 Interview Guide

The researcher conducted interviews on ICT officers and health records personnel. These are people the researcher believes would be sufficiently knowledgeable on the subject under study. The interviewees revealed adequate descriptions and understanding of the variables in the study since they are individuals who mostly interact with ISM.

3.6.3 Data Collection Process

The researcher acquired a license then use questionnaires and an interview guide to obtain data from the participants. The researcher used enumerators to gather data from participants at the public hospitals in Nairobi Metropolitan. Each study site had one enumerator. The researcher coached the enumerators on how to acquire data and the ethical requirements prior to handing them the questionnaires.

The questionnaire was administered personally to the hospitals' healthcare personnel. ICT officers and health record personnel was viewed as key respondents who would be interviewed using an interview guide. According to Maxfield & Babbie (2017), differentiated interviews can be integrated into any study as an additional data source. Therefore, the interview guide was administered to supplement the data obtained from the questionnaires. The interview guide produced both systematically measurable data and detailed qualitative information that was significantly enhanced the study. The interview guide provided an opportunity for the researcher to conduct in-depth questioning. Thus, it allowed the participants to share more information about Information Security Metrics.

3.7 Validity and Reliability

Validity of the tool means the apparatus can appraise that which it alleges to appraise. To increase validity, two apparatus were employed to evaluate the variables in the study. Reliability analysis was done through a pilot test to check for consistency of the tools for the study. The Cronbach Alpha was applied to test whether the variables under investigation met the threshold (Taber, 2018). Variables that achieved a Cronbach's alpha value of 0.70 or higher were retained for further analysis, as this threshold indicated acceptable internal consistency. In addition, a test–retest reliability assessment was conducted, and only variables with a correlation coefficient of at least 0.758 were considered reliable. This two-step screening ensured that the study proceeded with variables that met the required reliability standards.

The study employed methodological triangulation using different techniques of data acquisition, to ensure validity of findings (Cohen, Morrison, & Manion, 2018). This was beneficial because it allowed collection of more detailed data and verify the findings, which shall eventually raise validity. Data was obtained through questionnaires and semi structured interviews. For data analysis, qualitative and quantitative techniques of data shall be applied. The qualitative data collected complemented and clarified the quantitative findings by identifying common themes.

3.8 Pilot Study

The researcher performed an experimental study to pre-test the questionnaires on 38 deliberately selected participants from healthcare workers, ICT officers and health records personnel at Thika sub county level five hospital in Kiambu County to determine if the data gathered achieves the goals of the research. This is derived from the project by Hertzog (2008) who stated that an experimental sample ought to be 10% of the study's sample size. Data collected was analysed to identify any flaws and revise the questionnaire accordingly.

3.9 Data Management and Analysis

The researcher intends to obtain data daily from the field for a period not less than seven days. Enumerators submitted fully answered questionnaires to the researcher daily. Open-ended questions shall be encoded and recorded. Data cleaning was carried out to verify all questions have been answered. At the end of every day the researcher keyed in the acquired data to the Statistical Package for Social Sciences (SPSS) software for analysis. Data obtained through the interview guide was documented in note books and audio devices. Where necessary, data was transcribed and typed in word-for-word in MS Word. Subsequently, the data shall be due for thematic analysis, and shall be used together with the data collected through questionnaires.

Quantitative data was evaluated through illustrative and deductive statistics. Descriptive statistics were applied to arrange, summarize and transmit principal variables. The statistics to be utilized are percentages and statistical distributions. The impact of the independent variables on the dependent ones were examined through inferential statistics which included both correlation and regression analysis. Correlation analysis was used to test for association among the variables. These variables were measured at both nominal and ordinal levels, "1" indicated a strong positive association. "0" indicated no association at all while "-1" indicated a strong negative association. Age, years worked at the hospital and number of computers was calculated at interval level. A cross- tabulation evaluation of the variables was applied. The correlation analysis model took the form of:

$$\rho = 1 - \frac{6\sum d_i^2}{n(n^2-1)}$$

ρ=Pearson correlation

d_i = differences between x-variable and y-variable

$\sum d_i^2$= sum of the squared differences between x-and y- variables

n = sample size

The study further conducted simple regression analysis to assess the relationship between each independent variable against the dependent variable (patient safety). The following models were used to link the variables:

$$\mathbf{Y = \beta_0 + \beta_1 X_1 + \epsilon_{it}} \quad \text{.....3.1}$$

Y = Patient Safety

X_1 = Technical Components

$$\mathbf{Y = \beta_0 + \beta_2 X_2 + \epsilon_{it}} \quad \text{.....3.2}$$

Y = Patient Safety

X_2 = Security Controls

$$\mathbf{Y = \beta_0 + \beta_3 X_3 + \epsilon_{it}} \quad \text{.....3.3}$$

Y = Patient Safety

X_3 = Key Patient Safety Reporting Systems

$$\mathbf{Y = \beta_0 + \beta_4 X_4 + \epsilon_{it}} \quad \text{.....3.4}$$

Y = Patient Safety

X_4 = Legal Challenges

The variables of this study were operationalized and measured as shown in Table 3.1.

Table 3.1: Operationalization of Study Variables

Variable	Category	Operationalization	Measurement	Scale
Technical Components of Information Security Metrics (ISM)	Independent	Availability, functionality, and adequacy of technological infrastructure supporting ISM in	Composite mean score of Likert-scale items on technical	Interval

		public referral hospitals	components (1–5)	
ISM Security Controls	Independent	Safeguards and mechanisms that ensure confidentiality, integrity, and availability of patient data within ISM	Composite mean score of Likert-scale items on security controls (1–5)	Interval
ISM Reporting Systems	Independent	Systems and procedures used by healthcare facilities to record, report, and escalate ISM-related issues affecting patient safety	Composite mean score of Likert-scale items on reporting systems (1–5)	Interval
ISM Legal Aspects (Data Protection Compliance)	Independent	Legal requirements and patient rights governing data collection, consent, and confidentiality as guided by the Data Protection Act (2019)	Composite mean score of Likert-scale items on legal aspects (1–5)	Interval
Patient Safety (ISM-related Safety Outcomes)	Dependent	Level of patient protection from preventable medical errors arising from ISM practices	Composite index combining ISM incident responses (Yes/No coded 1/0), ISM use rating (1–4), and patient safety rating (1–4)	Interval / Ordinal (depending on analysis)

3.10 Ethical Considerations

Firstly, a letter of approval to collect data was sought from graduate school to allow for data collection. The researcher then sought an ethical approval letter from Kenyatta University Ethics Review Committee. Afterwards the researcher sought approval to carry out research from NACOSTI. The researcher sought ethical clearance from KNH-UON ERC and also

acquire permission to conduct the study from the facility administration. Respondents' approval was acquired prior to them being allowed to participate in the research. For the community considerations the researcher ensured that no harm (physical, psychological, emotional or social) occurred to the participants by selecting topics and methods that preclude any harm arising.

Participation was voluntary and a letter of informed consent was presented to ensure that there was no coercion or deception. Anonymity, confidentiality and privacy was observed in the entire study by not recording the participants' names and personal details in the questionnaires or interview forms. The participants had an assurance that the details presented were not be shared in a manner that could point to them. The researcher observed MOH guidelines on COVID-19 prevention measures at all times since the study was conducted between 2021 and 2022 when MOH guidelines on Covid-19 were still being observed in these facilities. The participants were briefed on the benefits of the information they share prior to engaging them in the interviews or distributing the questionnaires. Vulnerable groups like the elderly and children who could not defend their own rights were not be interviewed.

CHAPTER FOUR

DATA ANALYSIS AND INTERPRETATION

4.1 Introduction

The purpose of this study was to find out what challenges are experienced in the use of Information Security Metrics to improve patient safety at public referral hospitals in Nairobi Metropolitan. The study specifically sought to; find out which technical components of Information Security Metrics are in place and their effects in promoting patient safety, identify security controls that protects the Privacy, Integrity and Accessibility of data in Information Security Metrics in promoting patient safety, identify key patient safety reporting systems in Information Security Metrics that help in reducing medical errors and find out the legal challenges of using Information Security Metrics to promote patient safety in reference to the Kenyan Data Protection Act, No. 24 of 2019. This chapter presents the findings form the analysis including response rate, demographic characteristics, descriptive statistics and inferential statistics. The chapter covers the interpretations and discussion of the study findings which is done per study objectives. The study findings are based on data collected from three public hospitals in Nairobi Metropolitan: Kenyatta National Hospital, Spinal Injury Referral Hospital and Mathari National Teaching and Referral Hospital.

4.2 Response Rate

The response rate refers to the proportion of participants who complete and return a questionnaire out of the total sampled respondents. Response rate is necessary because it reflects the level of engagement and participation, helps assess the representativeness of the sample, reduces nonresponse bias, and ensures that the findings are reliable and generalizable to the broader population. The study targeted four referral hospitals in Nairobi Metropolitan, namely Kenyatta National Hospital, Spinal Injury Referral Hospital, Mathari National Teaching and Referral Hospital and Kenyatta University Teaching Referral and Research Hospital (KUTRRH). However, permission was not granted to collect data at KUTRRH with the management citing cessation of data collection in the hospital. The study therefore collected data from the other 3 hospitals with a total sample size of 288 respondents to whom questionnaires were administered. The response rate is shown in Table 4.1.

Table 4.1: Response Rate

Questionnaires	Frequency	Response Rate (%)
Returned	161	55.9
Unreturned	127	44.1
Total	288	100

The results in Table 4.1 shows that the response rate was 55.9% indicating that out of 288 questionnaires administered across the three referral hospitals, 161 were dully completed and returned. This low response rate is attributed to the challenges in accessing data and obtaining permissions. This response rate is considered adequate according to Mugenda and Mugenda (2003) who recommend a return rate of 50% as adequate for analysis and reporting. Therefore, the information provided in the research instruments provides sample representation for meaningful generalization.

4.3 Demographic Characteristics

Demographic characteristics of respondents refer to the specific personal and socio-economic attributes of individuals participating in a study. In this study demographic characteristics included: gender, age, professional body, education level, facility of operation, work experience and department of operation. The demographics were necessary for the discussion regarding the sample size composition. Table 4.2 summarizes the demographic characteristics.

Table 4.2: Demographic Characteristics

Demographic	Category	Frequency	Percentage
Gender	Male	83	51.6
	Female	78	48.4
	Total	**161**	**100**
Age	21-30 years	64	39.8
	31-40 years	53	32.9
	41-50 years	31	19.3
	51+ years	13	8.1
	Total	**161**	**100**
Professional Body	Nursing Officer	17	10.6
	Clinical Officer	26	16.1
	Community Oral Health Officer	3	1.9
	Dentist	19	11.8
	Medical Doctor	23	14.3
	Medical consultant specialist	18	11.2
	Laboratory Officer	4	2.5
	Physiotherapist/Occupational health	20	12.4
	Radiologist/Radiographer	7	4.3
	Pharmacist	24	14.9
	Total	**161**	**100**
Level of Education	Certificate Level	9	5.6
	Diploma	33	20.5
	Higher Diploma	18	11.2
	Undergraduate	74	46
	Masters	27	16.8
	Total	161	100
Current Hospital of Work	Kenyatta National Hospital	57	35.4

	Spinal Injury Referral Hospital	37	23
	Mathari National Teaching and Referral Hospital	67	41.6
	Total	**161**	**100**
Years worked in current Hospital	<1	12	7.5
	1-5 yrs.	115	71.4
	5-10 yrs.	17	10.6
	10-15 yrs.	13	8.1
	>15 yrs.	4	2.5
	Total	**161**	**100**
Department Working in Currently	Dental services	20	12.4
	Intensive care and theatre service	13	8.1
	Medical ward	18	11.2
	Surgical ward	16	9.9
	Medical records	31	19.3
	Pharmacy services	23	14.3
	Casualty and emergency services	16	9.9
	Medical imaging and diagnostics	11	6.8
	Maternity services	9	5.6
	Child health services	4	2.5
	Total	**161**	**100**

The demographic results in Table 4.2 depicts that there was nearly equal gender representation, with males representing 51.6% (83) and females accounting for 48.4% (78) of the respondents. This indicates a diverse perspective across genders in understanding the challenges related to Information Security Metrics in the context of patient safety. In addition, majority of respondents were within the age group of 21-30 years, accounting for 39.8% (64). This was followed by those in the 31-40 years age bracket, representing 32.9% (53). Respondents aged 41-50 years constituted 19.3% (31), and those over 51 years made up 8.1% (13). This distribution implies that the study sample was predominantly young to middle-aged, reflecting the workforce demographics in the healthcare sector within the Nairobi Metropolitan area.

In terms of professional body, the respondents were diverse in terms of their professional backgrounds. Clinical Officers were the most represented group, constituting 16.1% (26), followed by Pharmacists at 14.9% (24), and Medical Doctors at 14.3% (23). Nursing Officers made up 10.6% (17) of the sample, while other professionals such as Community Oral Health Officers, Dentists, Medical Consultant Specialists, Laboratory Officers, Physiotherapists, Occupational Health Workers, Radiologists, and Radiographers were also included in varying proportions. This distribution showcased a broad range of healthcare professionals, thus ensuring that the perspectives on Information Security Metrics were well-rounded.

Regarding highest educational qualifications, majority of respondents held an undergraduate degree (46%, 74), followed by those with a diploma (20.5%, 33). Respondents with a master's degree comprised 16.8% (27), while those with higher diplomas represented 11.2% (18). Only a small fraction of respondents had certificate level qualification (5.6%, 9). The high percentage of respondents with undergraduate and postgraduate qualifications indicates that majority of the participants had high levels of educational backgrounds, potentially contributing informed decisions on information security challenges.

In terms of the hospitals represented, Mathari National Teaching and Referral Hospital had the largest proportion of respondents at 41.6% (67), followed by Kenyatta National Hospital with 35.4% (57), and Spinal Injury Referral Hospital with 23% (37). The distribution across these hospitals ensured that a diverse range of experiences and challenges related to Information Security Metrics was captured across different healthcare settings within the Nairobi Metropolitan. Majority of these participants (71.4%, 115) had worked in their current hospital for between 1-5 years, indicating relatively recent experience in their current roles. A smaller percentage had worked for less than a year (7.5%, 12), while those with 5-10 years of experience constituted 10.6% (17). A limited number of respondents had 10-15 years (8.1%, 13) or more than 15 years (2.5%, 4) of experience in their current hospital. This shows that

most respondents had a moderate level of experience, potentially bringing fresh perspectives on current practices in information security.

The respondents were also asked to indicate they had education background in computer applications. Their responses were as shown in Figure 4.1.

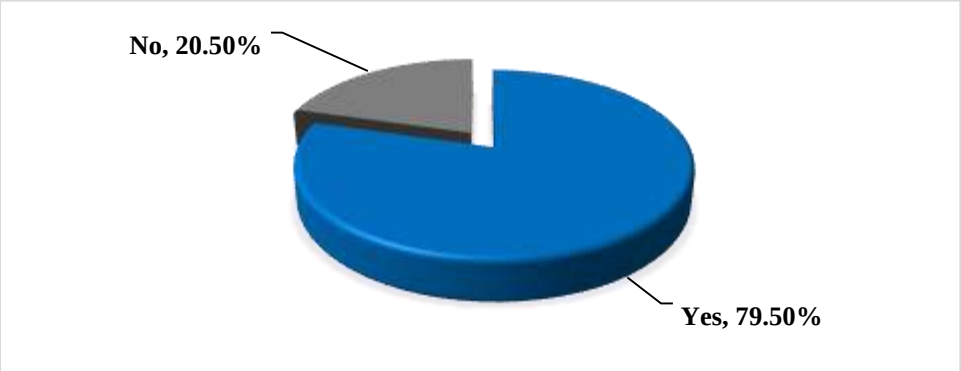


Figure 4.1: Education Background in Computer Applications

Based on the results, majority of the respondents (79.5%) reported having an educational background in computer applications, indicating a strong foundational knowledge in digital competencies relevant to Information Security Metrics. This suggests that most healthcare professionals in these hospitals are equipped to understand and engage with technical components that impact patient safety. However, the 20.5% without such a background may face challenges in effectively implementing and adhering to information security protocols. This gap imply there is need for targeted training and support to ensure all staff members can contribute to maintaining data privacy, integrity, and accessibility within the hospitals. The respondents who did not have educational background in computer applications were further asked if that affected how they interacted with ISM or not. There responses were as shown in Figure 4.2.

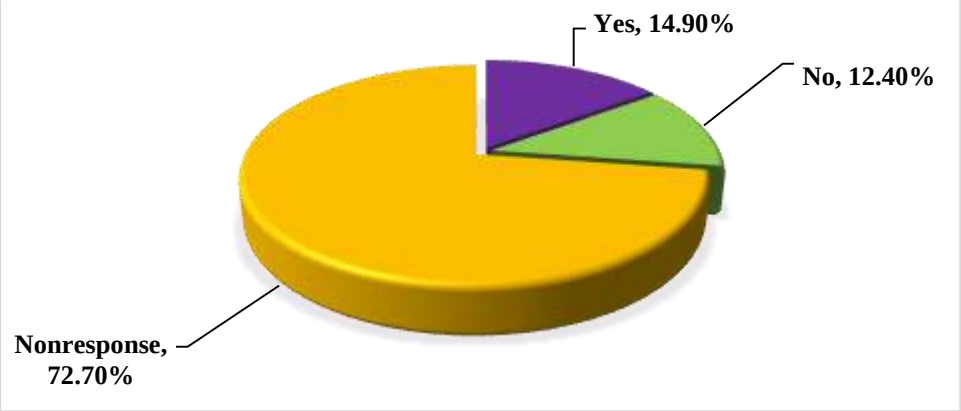


Figure 4.2: Effect of Lack of Educational Background in Computer Applications

A majority of respondents who lacked a background in computer applications did not respond to the question about its effect on their interaction with Information Security Metrics (ISM), with a high nonresponse rate of 72.7%. Of those who did respond, 14.9% felt their lack of computer education affected their interaction with ISM, while 12.4% did not perceive an effect. The high nonresponse rate suggests potential uncertainty or reluctance in acknowledging challenges related to ISM usage, which points to the need for further training or support for those lacking digital skills.

The respondents were also asked to indicate if they were holding any administrative positions at their healthcare facility or not. The responses were as shown in Figure 4.3.

Figure 4.3: Administrative Position

The results in Figure 4.3 depicts that majority of respondents (60.9%) did not hold administrative positions at their healthcare facility, while 39.1% did. This distribution implies that most of the respondents were primarily clinical or support staff, rather than involved in decision-making roles. Since administrative staff are often responsible for implementing and overseeing Information Security Metrics (ISM) policies, the perspectives from both administrative and non-administrative staff provided a balanced view on ISM practices and challenges. For the respondents who were holding administrative positions, they were asked to indicate if the position allowed them to make vital ISM decisions that help improve patient safety. Figure 4.4 shows their responses.

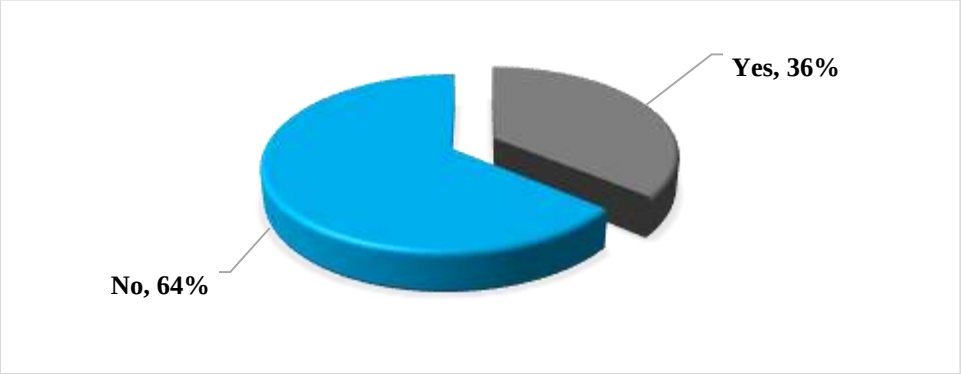


Figure 4.4: Position to Make Vital ISM Decisions

Majority of respondents in administrative positions (64%) indicated that their roles did not allow them to make vital decisions regarding Information Security Metrics (ISM) that would enhance patient safety, while only 36% felt empowered to influence these critical decisions. This disparity suggests a potential gap in decision-making authority within the healthcare facilities, which is likely to hinder the effective implementation of ISM practices necessary for

improving patient safety. The lack of involvement in crucial ISM decisions is likely to result in inadequate attention to data protection measures, ultimately impacting patient outcomes. This highlights the need for clearer lines of authority and responsibility, ensuring that those in administrative roles are equipped to make informed decisions regarding ISM. Additionally, creating collaboration between clinical and administrative staff may enhance the overall effectiveness of patient safety initiatives.

The respondents were further asked to indicate how they would rate the overall use of ISM in their hospitals. The responses were as shown in Figure 4.5.

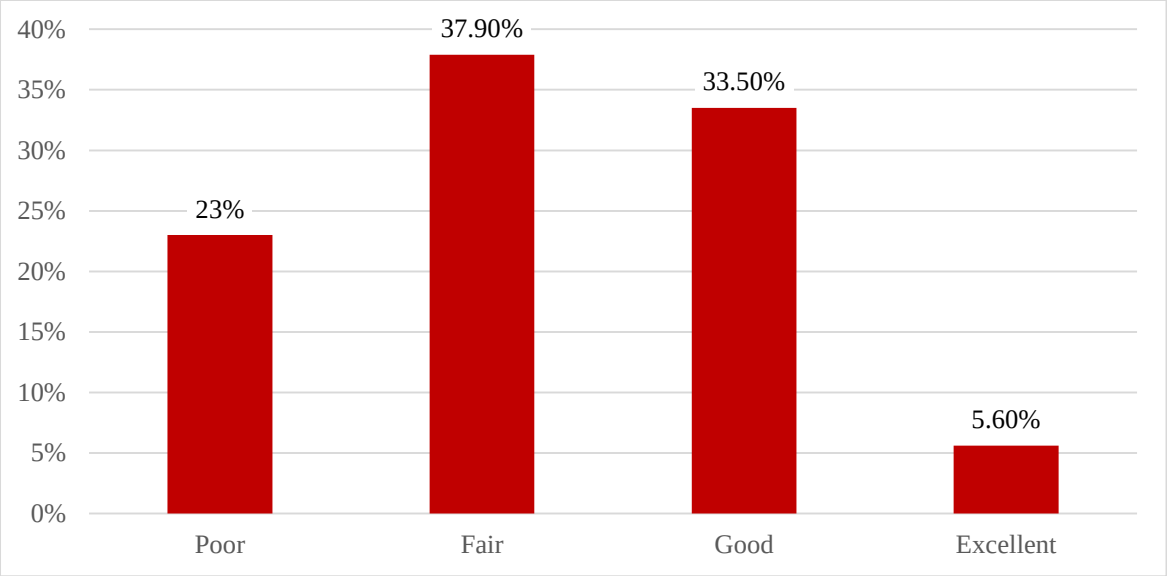


Figure 4.5: Rating the Overall Use of ISM

The respondents provided a mixed assessment of the overall use of Information Security Metrics (ISM) in their hospitals, with 37.9% rating it as fair, 33.5% as good, 23% as poor, and only 5.6% deeming it excellent. This distribution indicates that while a considerable portion of

the staff recognizes some positive aspects of ISM implementation, a good number (23%) find it lacking, which may reflect ongoing challenges in effectively using these metrics to enhance patient safety. The predominance of "fair" ratings suggests that while there are efforts in place, there is some room for improvement in ISM practices. Additionally, the low percentage of respondents rating ISM as excellent points to the need for targeted initiatives to enhance the effectiveness of information security protocols, ensuring that they adequately safeguard patient data and improve overall safety outcomes.

Regarding issues faced, the respondents were asked to indicate the types of ISM issues they had encountered in their clinical practices in their respective hospitals over the previous 12 months. The responses were as shown in Table 4.3.

Table 4.3: Types of ISM Issues Encountered

Statement	Yes	No
Technical glitch in data collection software	15.50%	84.50%
Missing patient information in data collection software	41.60%	58.40%
Incorrect patient information in data collection software	34.80%	65.20%
Ads and unnecessary information while using data collection software	34.80%	65.20%
Inability to access patient information despite having clearance	66.70%	33.30%

The results in Table 4.3 shows that 15.5% of the respondents reported experiencing technical glitches in their data collection software, suggesting that while these issues may exist, they are not universally pervasive. However, 84.5% who did not encounter this issue indicates a level of stability in the software performance for most users. The results however shows that 41.6% of respondents encountered missing patient information, with 58.4% reporting they did not. This indicates a critical issue that is likely to directly affect patient safety and care continuity, as incomplete records can lead to misunderstandings and medical errors. The implications of

missing data necessitate a thorough review of data entry protocols and software capabilities to ensure that patient information is accurately captured and maintained.

Similarly, 34.8% of respondents reported encountering incorrect patient information, while 65.2% did not. This suggests that discrepancies in patient data are a notable issue that could lead to significant clinical risks, such as inappropriate treatments or medication errors. Addressing these inaccuracies is crucial, emphasizing the need for regular audits and updates of the data collection system to minimize errors and improve data integrity. The presence of ads and unnecessary information in the data collection software was reported by 34.8% of respondents. This issue can detract from the user experience, making it harder for healthcare providers to locate essential patient information quickly. Streamlining the interface to reduce clutter can enhance usability, allowing clinicians to focus more on patient care rather than navigating irrelevant information.

Moreover, most (66.7%) of the respondents faced challenges accessing patient information despite having clearance. This points to serious flaws in the information security and access protocols that may prevent timely and necessary access to critical patient data. The implications of such access issues can be severe, potentially leading to delays in treatment and adverse patient outcomes. Therefore, it is imperative for hospitals to evaluate and enhance their access control mechanisms, ensuring that authorized personnel can retrieve necessary information without unnecessary barriers.

Finally, the respondents were asked to indicate what they would attribute as the most common cause of medical errors concerning ISM in their healthcare facilities. Their responses were as shown in Table 4.4.

Table 4.4: Most Common Cause of Medical Errors

Cause	Frequency	Percentage

Patient information not available at the right time	18	11.2
Lack of managerial support in using ISM	32	19.9
Inadequate ISM skills among healthcare workers	48	29.8
Inadequate ISM reporting systems	25	15.5
Lack of ISM culture in the organization	38	23.6
Total	**161**	**100**

The results show that the most common cause attributed to medical errors was the inadequate ISM skills among healthcare workers, with 29.8% (48) identifying this issue. This finding indicates a critical gap in the training and education of healthcare personnel regarding ISM practices. Without sufficient knowledge and skills, healthcare workers may struggle to effectively utilize ISM tools, leading to errors in data entry, retrieval, and interpretation. Following closely, 23.6% (38) pointed to a lack of ISM culture within the organization as a contributing factor to medical errors. This indicates that, beyond individual skills, the overall organizational attitude towards ISM plays a significant role in shaping practices. A weak ISM culture may result in insufficient prioritization of data security and information accuracy, further exacerbating the risk of medical errors. This finding suggests that creating a strong ISM culture where data security is valued and integrated into daily operations can help mitigate errors and enhance patient safety.

Additionally, the lack of managerial support in using ISM was noted by 19.9% (32 respondents) as another important cause of medical errors. This implies that without strong leadership backing the implementation of ISM practices, healthcare workers may feel unsupported or unsure about adhering to information security protocols. Leadership commitment is vital for promoting best practices in ISM, and organizations may need to engage management in developing clear policies, providing resources, and fostering an environment where ISM is prioritized.

Inadequate ISM reporting systems were cited by 15.5% (25) as a common cause of medical errors. This suggests that existing systems may not effectively capture or relay critical patient information, leading to lapses in care. The design and functionality of reporting systems are crucial for ensuring that healthcare professionals can access accurate and timely information. Improving these systems can significantly reduce the likelihood of errors occurring due to miscommunication or lack of access to patient data. Finally, only 11.2% (18) indicated that patient information not being available at the right time contributed to medical errors. While this was the least common cause identified, it remains an important issue. Timeliness in accessing patient data is crucial for effective decision-making in clinical settings. Delays in obtaining essential information can hinder the quality of care and potentially lead to adverse outcomes.

4.4 Technical Components of Information Security Metrics and Patient Safety

The first objective of the study was to examine the technical components of information security metrics and their effects in promoting patient safety.

4.4.1 Descriptive Statistics

The respondents were therefore asked to indicate their levels of agreements with statements concerning technical components about their hospitals. The study used a scale of 1-5 such that 1-strongly disagree, 2-disagree, 3-neutral, 4-agree, 5-strongly agree. Table 4.5 shows the descriptive statistics results.

Table 4.5: Descriptive Statistics on Technical Components of ISM

Statement	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Std. Dev.
This healthcare facility has a data collection software where patient data is collected and stored	1.90%	21.10%	19.90%	43.50%	13.70%	3.46	1.03

The healthcare staff in this hospital are adequately trained in use of ISM	15.60%	33.10%	18.80%	24.40%	8.10%	2.76	1.22
The hospital management prioritizes use of ISM in promoting patient safety	11.20%	31.10%	26.10%	15.50%	16.10%	2.94	1.25
For this health care facility, computers, laptops, Ipads are adequately available for the access and storage of patient information	3.10%	32.10%	21.40%	27.70%	15.70%	3.21	1.15
For this health care facility, a backup generator is available to power up computers that are used in storage of patient information	1.30%	5.00%	23.90%	49.10%	20.80%	3.83	0.86
This healthcare facility has stand by technicians that handle any technical issues arising in the use of ISM	12.70%	38.20%	9.60%	23.60%	15.90%	2.92	1.33
This healthcare facility addresses technical issues regarding ISM promptly and swiftly	14.30%	36.00%	19.30%	24.20%	6.20%	2.72	1.16
There is a culture of organizational learning and evidence based decision making from patient data collected in this hospital	10.60%	29.80%	31.10%	23.00%	5.60%	2.83	1.07
In this healthcare facility culture of using ISM is practiced	12.60%	27.00%	30.80%	23.30%	6.30%	2.84	1.11
Overall Mean						**3.057**	

The results presented in Table 4.5 indicate varying levels of agreement among respondents regarding the technical components of Information Security Metrics (ISM) in their healthcare facilities. A majority of respondents (57.2%) agreed that their healthcare facility had data collection software where patient data was collected and stored. The mean score of 3.46 suggests a positive perception of the availability of such software, indicating that most respondents recognized its presence as a fundamental tool for managing patient data.

In contrast, a majority of respondents (48.7%) disagreed that healthcare staff were adequately trained in the use of ISM, with a mean score of 2.76. This reflects a significant concern regarding the competency of staff in managing ISM tools, which may hinder effective patient care and safety. The majority of respondents (42.3%) disagreed that hospital management prioritized the use of ISM in promoting patient safety, as indicated by a mean score of 2.94. This lack of prioritization could contribute to insufficient support and resources for effective ISM implementation, ultimately affecting patient outcomes.

A majority of respondents (59.8%) disagreed that adequate computers, laptops, and iPads were available for accessing and storing patient information, with a mean score of 3.21. This indicates that the necessary technological infrastructure may be lacking, potentially impeding data management processes. In a more positive finding, a majority (69.9%) agreed that a backup generator was available to power computers used in the storage of patient information, reflected by a mean score of 3.83. This suggests that there are contingency measures in place to ensure data accessibility during power outages.

The majority of respondents (50.5%) disagreed that standby technicians were available to handle technical issues arising in the use of ISM, with a mean score of 2.92. This indicates a significant gap in immediate technical support, which could exacerbate issues faced by healthcare staff in utilizing ISM tools effectively. A majority of respondents (50.3%) disagreed that technical issues regarding ISM were addressed promptly and swiftly, as indicated by a mean score of 2.72. This reflects a critical area for improvement, as delays in addressing technical problems can compromise the reliability of ISM.

Moreover, majority of the respondents (40.4%) disagreed that a culture of organizational learning and evidence-based decision-making from patient data existed in their hospital, with a mean score of 2.83. This lack of a learning culture may hinder the effective use of collected data to inform clinical practices and improve patient safety. Finally, a majority (39.6%)

undecided on the statement that a culture of using ISM was practiced in the healthcare facility, as reflected by a mean score of 2.84. This suggests that the integration of ISM into daily operations is not yet fully realized, which may limit its effectiveness in enhancing patient care.

Thematic Analysis

During interviews with ICT officers and health records personnel, respondents were asked to describe the data collection methods employed in their hospitals. Most respondents indicated that a variety of methods were being used to ensure detailed data collection. These methods include direct patient interviews, the use of Electronic Health Record (EHR) systems, and standardized forms for data entry. They emphasized the importance of integrating both qualitative and quantitative approaches to data collection to support patient safety and inform care decisions effectively. Respondent N1 explained that:

> *"Data collection in our hospital involves multiple approaches tailored to the type of information needed. Direct patient interviews provide qualitative insights, while standardized forms and EHR systems enable structured, quantitative data collection. This combination ensures a holistic approach to understanding and managing patient needs."*

When asked about the data collection software used for managing patient data, respondents noted that the hospitals primarily rely on EHR systems. Specifically, they mentioned the use of the District Health Information System (DHIS-2) for managing health data, complemented by custom-built applications tailored to the specific needs of various departments. These systems, according to respondents, play a crucial role in streamlining data management, facilitating analysis, and ensuring secure storage, thereby enhancing patient safety protocols. Respondent N2 stated:

"Our hospital relies heavily on the DHIS-2 for managing health data across departments. This system, along with custom-built applications, allows us to collect, analyze, and store data efficiently. By integrating these tools, we've significantly improved our ability to make data-driven decisions and support patient safety initiatives."

The responses from ICT officers and health records personnel points to the critical role of diverse data collection methods and advanced software in enhancing healthcare operations. The integration of qualitative and quantitative approaches through tools like EHR systems and DHIS-2 ensures that data collection is both comprehensive and efficient. However, these responses also indicate the need for continuous improvement in tailoring these systems to meet the specific needs of hospitals, ensuring that all departments are adequately supported in their data collection and management efforts. This aligns with assertions by scholars such as Mynbayeva, Sadvakassova, and Akshalova (2018), who emphasize the importance of robust systems and tools in managing information effectively to promote safety, efficiency, and quality in service delivery.

4.4.2 The Exploratory Factor Analysis

The Exploratory Factor Analysis was conducted using Principal Axis Factoring with Varimax rotation, and two main factors were extracted. The data presented in tables 4.6. 4.7 and 4.8.

Table 4.6: Communalities

Statement	Initial	Extraction
This healthcare facility has a data collection software where patient data is collected and stored.	0.491	0.441
The healthcare staff are adequately trained in use of ISM.	0.645	0.637
The hospital management prioritizes use of ISM in promoting patient safety.	0.799	0.892
Computers, laptops, iPads are adequately available for the access and storage of patient information.	0.539	0.606
A back-up generator is available to power up computers that are used in storage of patient information.	0.328	0.452

This healthcare facility has stand by technicians to deal with technical issues arising in the use of ISM.	0.617	0.688
This healthcare facility addresses technical issues regarding ISM promptly and swiftly.	0.707	0.702
There is a culture of organizational learning and evidence-based decision-making from patient data collected in this hospital.	0.677	0.708

Communalities values, shown in Table 4.6, indicate the extent to which each variable is represented by the factors extracted. Most communalities range from moderate to high, with "hospital management prioritizes ISM" showing a particularly high extraction value (initial = 0.799, extraction = 0.892), suggesting that this variable is strongly associated with ISM practices. High communalities across several components affirm that the factors extracted in EFA adequately capture the shared variance, thereby validating the factor structure.

Table 4.7: Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.828	60.355	60.355	4.503	56.286	56.286	3.214	40.179	40.179
2	1.036	12.955	73.310	.623	7.782	64.068	1.911	23.889	64.068
3	.629	7.863	81.172						
4	.462	5.770	86.942						
5	.411	5.135	92.078						
6	.277	3.464	95.541						
7	.209	2.613	98.154						
8	.148	1.846	100.000						

Extraction Method: Principal Axis Factoring

Table 4.7 reveals that two factors extracted through Principal Axis Factoring explain approximately 64.07% of the total variance in the ISM components. Factor 1 accounts for 40.18% of the variance, while Factor 2 explains an additional 23.89%. This cumulative variance is sufficiently high to capture meaningful insights, suggesting that the two-factor model provides a robust representation of the ISM structure within these healthcare facilities.

Table 4.8: Rotated Factor Matrix

Statement	Factor 1	Factor 2
This healthcare facility has a data collection software where patient data is collected and stored	0.664	-0.010
The healthcare staff are adequately trained in use of ISM	0.758	-0.250
The hospital management prioritizes use of ISM in promoting patient safety	0.911	-0.247
Computers, laptops, iPads are adequately available for the access and storage of patient information	0.715	0.308
A back-up generator is available to power up computers that are used in storage of patient information	0.478	0.473
This healthcare facility has stand by technicians to deal with technical issues arising in the use of ISM	0.767	0.315
This healthcare facility addresses technical issues regarding ISM promptly and swiftly	0.836	-0.053
There is a culture of organizational learning and evidence-based decision making from patient data collected in this hospital	0.793	-0.280

The Rotated Factor Matrix, shown in Table 4.8, shows the factor structure, allowing for distinct interpretation of each factor. After Varimax rotation, Factor 1 primarily captures items related to organizational commitment to ISM, while Factor 2 encompasses components linked to infrastructure and technical support.

Discussion of EFA Findings and Descriptive Analysis Linkage

The EFA findings are consistent with the descriptive statistics by identifying two overarching themes (factors) within ISM components: management and organizational commitment and infrastructure and technical support. Factor 1, reflecting management and organizational commitment, includes high loadings for items such as "hospital management prioritizes ISM" (loading = 0.887) and "culture of evidence-based decision-making" (loading = 0.810). These items emphasize the critical role of a supportive management structure, which reinforces the descriptive finding of moderate-to-low scores on management prioritization. This gap in leadership commitment could undermine ISM’s integration into safety practices, suggesting that increased management support would likely enhance ISM’s effectiveness in safeguarding patient data.

Factor 2, representing infrastructure and technical support, captures components essential for ISM functionality, such as availability of devices (loading = 0.663), backup generators (loading = 0.662), and standby technicians for ISM issues (loading = 0.700). Descriptive analysis highlighted that while some infrastructural elements like backup generators are well-implemented, other areas, such as technical support and prompt issue resolution, scored lower. The factor analysis confirms the importance of a stable infrastructure and responsive technical support, underscoring that a robust ISM system requires both reliable equipment and a rapid response to technical challenges.

By examining both the descriptive statistics and EFA findings, a comprehensive view of ISM implementation within healthcare facilities emerges. The descriptive statistics reveal individual ISM components' strengths and weaknesses, while the EFA consolidates these into two critical dimensions. The findings suggest that while infrastructure may be relatively well-established, challenges remain in organizational commitment, staff competency, and technical support responsiveness. Addressing these gaps, particularly in management prioritization and technical responsiveness, could significantly enhance ISM's role in promoting patient safety.

4.5 Security Controls

The second objective of the study was to identify the security controls that protect the Privacy, Integrity and Accessibility of data in Information Security Metrics in promoting patient safety. This section presents descriptive, correlation and regression analysis results.

4.5.1 Descriptive Statistics

The respondents were asked to indicate their levels of agreements with statements concerning security controls that protects the privacy, integrity and accessibility of data in Information Security Metrics in promoting patient safety. The study used a scale of 1-5 such that 1-strongly

disagree, 2-disagree, 3-neutral, 4-agree, 5-strongly agree. Table 4.9 shows the descriptive statistics results.

Table 4.9: Descriptive Statistics on Security Controls

Statement	Strongly disagree	Disagree	Neutral	Agreed	Strongly Agreed	Mean	Std. Dev.
In this healthcare facility, it is okay to share computer passwords with others	15.40%	16.50%	12.70%	20.90%	7.00%	2.85	1.33
In this healthcare facility the computers are firewall enabled	0.80%	4.60%	36.00%	31.80%	3.70%	3.4	0.83
In this healthcare facility the computers have an up to date anti-virus	0.80%	11.10%	25.40%	33.00%	5.10%	3.37	0.94
This healthcare facility has proper system access control mechanisms like user accounts	0.00%	1.20%	11.60%	53.80%	13.20%	3.96	0.69
In this facility patient data is adequately protected from illegal access and accidental loss	0.00%	6.00%	24.30%	28.30%	17.60%	3.73	0.94
There are security controls present that protect data storage assets from theft and hacking	1.60%	8.60%	20.00%	34.10%	10.20%	3.51	1.02
Overall Mean						**3.470**	

The descriptive statistics results in Table 4.9 indicate varied responses concerning security controls that protect the privacy, integrity, and accessibility of data in promoting patient safety. The most of the respondents (35.9%) disagreed with the statement that it is acceptable to share computer passwords with others within the healthcare facility (mean = 2.85, SD = 1.33). This suggests that most participants recognized the importance of safeguarding passwords to maintain data security. Regarding the presence of firewalls, the slightly more than a third of the respondents (35.5%) agreed that computers in the facility were firewall-enabled (mean = 3.4, SD = 0.83). This indicates a generally positive stance towards the existence of firewalls as a security measure, although a considerable portion remained neutral. Similarly, the most of

the respondents agreed that computers had up-to-date antivirus software (38.1%, mean = 3.37, SD = 0.94), indicating recognition of antivirus programs as essential in maintaining data security.

When asked about system access control mechanisms such as user accounts, majority (67%) agreed that the facility had proper system access controls in place (mean = 3.96, SD = 0.69). The relatively high mean and low standard deviation demonstrate both strong consensus and confidence in access control mechanisms being well established. Likewise, most of the respondents (45.9%) agreed that patient data was adequately protected from illegal access and accidental loss (mean = 3.73, SD = 0.94), implying that there were effective measures to secure patient information.

The statement on protecting data storage assets from theft and hacking received agreement from 44.3% of respondents (mean = 3.51, SD = 1.02), suggesting that there was a reasonable level of confidence in the measures implemented to secure data storage assets. Generally, the mean score across all statements was 3.47, indicating that, on average, participants leaned towards agreeing that security controls are in place to protect data privacy, integrity, and accessibility, thereby promoting patient safety. The findings imply that even though there are generally positive perceptions of the security controls in place within the healthcare facility, there is still room for improvement, especially in areas with notable neutral responses or high standard deviations, which suggest some uncertainty or lack of consensus among respondents.

Thematic Analysis

During interviews with ICT officers and health records personnel, respondents were asked to describe the security procedures in place to protect patient data. The respondents outlined several measures implemented by the hospital to safeguard data. These include strict access controls, encryption of sensitive data, and regular security audits, which they identified as the

cornerstone of their data protection strategy. They also emphasized the importance of ongoing staff training on data protection protocols to maintain the confidentiality and integrity of patient information. Respondent N5 explained:

> *"Ensuring patient data security requires a multi-faceted approach. We rely on strict access controls and encryption to limit unauthorized access, while regular security audits help us identify and address vulnerabilities. Staff training is also critical in maintaining data protection standards."*

The interviewees further confirmed that the hospital conducts comprehensive training programs for healthcare staff focusing on Information Security Metrics (ISM) to promote patient safety. These training sessions are aimed at equipping personnel with the skills necessary to use ISM tools effectively, while reinforcing the importance of data security in their daily operations. Respondent N7 noted:

> *"Our hospital prioritizes regular training sessions to ensure that all healthcare staff are familiar with ISM tools and understand their role in safeguarding patient data. These sessions not only enhance technical skills but also foster a culture of accountability and awareness regarding data protection."*

The responses indicates the hospital's proactive approach to data security, combining technical measures with human resource development to address potential risks. Through implementation of effective access controls, encryption, and regular audits, alongside staff training initiatives, the hospital ensures a strong framework for protecting patient data and promoting patient safety. These efforts align with best practices in information security, demonstrating the hospital's commitment to integrating technology and workforce readiness in its data protection strategy.

4.5.2 The Exploratory Factor Analysis

The study sought to identify security controls that protects the Privacy, Integrity and Accessibility of data in Information Security Metrics in promoting patient safety. Exploratory Factor Analysis was conducted using Principal Axis Factoring with Varimax rotation, and the extraction results are shown in tables 4.10. 4.11 and 4.12.

Table 4.10: Communalities

Statement	Initial	Extraction
In this healthcare facility, it is okay to share computer passwords with others	0.812	0.339
In this healthcare facility, the computers are firewall-enabled	0.943	0.697
In this healthcare facility, the computers have an up-to-date anti-virus	0.971	0.720
This healthcare facility has proper system access control mechanisms like user accounts	0.653	0.290
In this facility, patient data is adequately protected from illegal access and accidental loss	0.857	0.733
There are security controls present that protect data storage assets from theft and hacking	0.921	0.825

The results of the Exploratory Factor Analysis, conducted to identify key security controls that support the privacy, integrity, and accessibility of data within Information Security Metrics, indicated varied levels of communalities across the statements assessed. The the statement regarding the facility's firewall-enabled computers showed a high level of extraction at 0.697, suggesting that firewall protections were integral to safeguarding data in this context. Similarly, the presence of up-to-date anti-virus software demonstrated a strong communal value of 0.720, emphasizing its role in maintaining data integrity and security.

The highest extraction value, 0.825, was associated with security controls to protect data storage assets from theft and hacking, underscoring its critical importance in ensuring data confidentiality and resilience against external threats. In contrast, system access control mechanisms, such as user accounts, had a lower extraction value of 0.290, indicating that while

they contributed to overall data security, they do not have as much impact as other controls within this healthcare setting. The findings suggests that tangible protections, such as firewalls, anti-virus software, and theft prevention measures, were pivotal elements in promoting patient safety by preserving data security, whereas other measures, though valuable, may have played a less important role in the security framework analyzed.

Table 4.11: Total Variance Explained

Compo-nent	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Vari-ance	Cumulative %	Total	% of Vari-ance	Cumulative %
1	3.605	60.088	60.088	3.605	60.088	60.088
2	0.881	14.685	74.773			
3	0.813	13.548	88.321			
4	0.28	4.659	92.98			
5	0.25	4.161	97.141			
6	0.172	2.859	100			

Extraction Method: Principal Axis Factoring

Table 4.11 reveals that a single main factor extracted through Principal Axis Factoring accounts for approximately 60.09% of the total variance in the security control components, with an initial eigenvalue of 3.605. This high percentage of variance captured by the first factor suggests that it provides a strong and cohesive representation of the primary security controls influencing patient safety in the facility. Although additional components were identified, none contributed significantly to the cumulative variance, with the second component accounting for only 14.69% and subsequent factors each explaining less than 14%. This one-factor model indicates a dominant dimension, indicating that a unified approach to security controls effectively explains the core aspects of data privacy, integrity, and accessibility in this healthcare setting.

Table 4.12: Rotated Factor Matrix

Statement	Factor 1
In this healthcare facility, it is okay to share computer passwords with others	-0.582
In this healthcare facility the computers are firewall enabled	0.835
In this healthcare facility the computers have an up to date anti-virus	0.849
This healthcare facility has proper system access control mechanisms like user accounts	0.539
In this facility patient data is adequately protected from illegal access and accidental loss	0.856
There are security controls present that protect data storage assets from theft and hacking	0.908

The Rotated Factor Matrix, presented in Table 4.11, shows a clear factor structure, allowing for interpretation of Factor 1. After Varimax rotation, Factor 1 mainly captures items related to security measures that safeguard data privacy, integrity, and accessibility. Specifically, high loadings on statements such as firewall-enabled computers (0.835), up-to-date anti-virus software (0.849), data protection from unauthorized access (0.856), and security controls to prevent theft and hacking (0.908) emphasize the facility's technical measures to secure patient data. In contrast, the negative loading on password-sharing (-0.582) suggests that such practices detract from effective data security within the facility. This factor thus represents a unified approach to technical and procedural controls aimed at maintaining data security within the healthcare environment.

Discussion of EFA Findings and Descriptive Analysis Linkage

The EFA findings are in tandem with the descriptive statistics, revealing a central theme within the security controls focused on technical and procedural measures to protect patient data privacy, integrity, and accessibility. Factor 1 primarily encompasses technical security controls, as evidenced by high loadings on items such as "firewall-enabled computers" (loading = 0.835), "up-to-date anti-virus software" (loading = 0.849), and "security controls to prevent theft and hacking" (loading = 0.908). These loadings indicates the facility's emphasis on tangible technological protections, consistent with the descriptive statistics that show positive

responses towards the presence of firewall and anti-virus protections. Additionally, the descriptive statistics reflect that the majority of respondents agreed on the importance of protecting patient data from illegal access, as shown by a high mean score on statements related to data security measures, further reinforcing Factor 1's focus on technical controls.

The lower extraction value for "system access control mechanisms" (loading = 0.539) in EFA corresponds with the relatively neutral descriptive responses in areas like password-sharing, indicating that access control practices may be less stringent or inconsistently applied within the facility. Similarly, there was negative loading on password-sharing (-0.582) in EFA indicating that password security practices are perceived as hindrance to overall data security, a sentiment echoed in the descriptive analysis where many respondents disagreed with the acceptability of sharing passwords.

Through the synthesis of both the descriptive analysis and EFA results, a comprehensive picture emerges of the data security environment in this healthcare setting. The descriptive statistics underscore individual security practices, with varying levels of respondent confidence, while the EFA consolidates these into a single factor centered on technical controls. This linkage suggests that while foundational security controls are relatively effective, there are areas for improvement in procedural practices, such as access control consistency and staff adherence to password management protocols. Improving procedural adherence, alongside maintaining technical security measures, are further able to strengthen data protection, thereby promoting patient safety in the facility.

.

4.6 Patient Safety Reporting Systems in Information Security Metrics

The third objective of this study was to identify key patient safety reporting systems in Information Security Metrics that help reduce medical errors. This section discusses descriptive statistics, correlation analysis and regression analysis.

4.6.1 Descriptive Statistics

The respondents were asked to indicate their levels of agreements with statements concerning key patient safety reporting systems in Information Security Metrics that help in reducing medical errors. The study used a scale of 1-5 such that 1-strongly disagree, 2-disagree, 3-neutral, 4-agree, 5-strongly agree. Table 4.13 shows the descriptive statistics results.

Table 4.13: Descriptive Statistics on Patient Safety Reporting Systems

Statement	Strongly disagree	Disagree	Neutral	Agreed	Strongly Agreed	Mean	Std. Dev.
In this hospital, healthcare workers are provided with conducive environment for reporting ISM incidences that affect patient safety	6.90%	35.60%	16.30%	33.10%	8.10%	3.00	1.14
The hospital management has invested in reporting systems that capture ISM related issues	14.90%	36.00%	26.10%	18.00%	5.00%	2.62	1.1
In this healthcare facility reporting of ISM related issues is mandatory	7.50%	41.00%	26.70%	21.70%	3.10%	2.72	0.99
Hospital staff are alerted promptly when data software are undergoing upgrades in their department	9.30%	25.50%	22.40%	32.90%	9.90%	3.09	1.16
The hospital management encourages reporting of ISM related issues	5.60%	37.30%	28.00%	23.00%	6.20%	2.87	1.03
In this healthcare facility there is a targeted patient safety incident	9.30%	34.20%	28.60%	23.60%	4.30%	2.8	1.04

report procedure for ISM related issues							
In this healthcare facility hospital management uses the reported cases to make evidence based decisions	7.50%	21.10%	39.80%	25.50%	6.20%	3.02	1.01
Overall Mean						**2.874**	

The results in Table 4.13 indicate varied responses concerning key patient safety reporting systems in Information Security Metrics (ISM) that help reduce medical errors. For the statement regarding whether healthcare workers are provided with a conducive environment for reporting ISM incidents affecting patient safety, majority of the respondents disagreed (42.5%), with a mean of 3.00 and a standard deviation of 1.14. This suggests that a significant portion of participants did not perceive the environment as supportive for reporting safety incidents, indicating potential barriers in fostering an open reporting culture. In addition, majority of the respondents disagreed that the hospital management has invested in reporting systems that capture ISM-related issues (50.9%, mean = 2.62, SD = 1.1), pointing to a perceived lack of adequate investment in systems that facilitate incident reporting. Similarly, 48.5% of respondents disagreed that reporting of ISM-related issues is mandatory in their healthcare facility (mean = 2.72, SD = 0.99), implying a lack of enforced protocols for reporting, which could impact the frequency and reliability of safety incident submissions.

When asked if hospital staff are promptly alerted about software upgrades, responses were more balanced, but the majority agreed (42.8%, mean = 3.09, SD = 1.16), indicating a relatively positive perception of communication regarding software changes. However, despite this agreement, the variability reflected in the standard deviation suggests some inconsistency in how promptly staff receive alerts. Regarding whether the hospital management encourages reporting of ISM-related issues, most respondents disagreed (42.9%, mean = 2.87, SD = 1.03), indicating that management's encouragement may be perceived as insufficient. This is

supported by the responses to the existence of a targeted patient safety incident report procedure for ISM-related issues, where the majority disagreed (43.5%, mean = 2.80, SD = 1.04). Such responses suggest a perceived gap in specific procedures aimed at addressing ISM issues effectively.

Finally, on whether the reported cases are used by the hospital management to make evidence-based decisions, majority were neutral (39.8%, mean = 3.02, SD = 1.01), suggesting a level of uncertainty or lack of clarity among respondents about how management utilizes reported data to inform decision-making. The overall mean score of 2.874 indicates that, on average, participants were undecided concerning the presence and effectiveness of patient safety reporting systems. These results suggest that there may be challenges related to establishing a culture of open reporting, investing in effective reporting systems, and using reported data to drive improvements. Addressing these areas could be vital for enhancing ISM reporting and, subsequently, patient safety.

Thematic Analysis

In addition, interviews were conducetd to support the above descriptive findings. During interviews with ICT officers and health records personnel, respondents were asked to discuss the availability of updated and on-site refresher courses for healthcare staff. The respondents noted that periodic training sessions are conducted to keep staff informed about the latest technologies and data management practices. However, they emphasized the need for more frequent and comprehensive training sessions to keep pace with the rapid advancements in healthcare technology. Respondent N3 explained:

> *"While periodic training sessions are beneficial, the fast-changing nature of technology in healthcare demands more regular and in-depth refresher courses.*

Continuous education is essential to maintaining effective Information Security Metrics (ISM) practices and ensuring patient safety."

When asked about the challenges encountered in using ISM to improve patient safety, the interviewees highlighted several critical issues. These included insufficient training resources, a lack of integration between different data systems, and inadequate technical support for resolving ISM-related problems. Additionally, they pointed out that gaps in management support for data security initiatives hinder the effective implementation of ISM, which can adversely affect patient safety outcomes. Respondent N6 noted:

"Challenges such as limited training resources and fragmented data systems make it difficult to fully implement ISM. Moreover, stronger management support is needed to drive these initiatives and ensure their success in improving patient safety."

The responses shows the importance of addressing both educational and operational challenges in ISM implementation. While periodic training provides a foundation, more frequent and tailored sessions are necessary to keep healthcare staff equipped with the latest skills. Additionally, resolving system integration issues, enhancing technical support, and securing stronger management commitment are critical steps to optimizing ISM's potential to enhance patient safety. These findings highlight the need for a comprehensive approach to overcoming barriers in ISM implementation to achieve sustainable improvements in healthcare outcomes.

4.6.2 The Exploratory Factor Analysis

The third objective of this study was identify key patient safety reporting systems in Information Security Metrics that help in reducing medical errors. Exploratory Factor Analysis was conducted using Principal Axis Factoring with Varimax rotation, and the extraction results are shown in tables 4.14. 4.15 and 4.16.

Table 4.14: Communalities

Statement	Initial	Extraction
In this hospital, healthcare workers are provided with conducive environment for reporting ISM incidences that affect patient safety	1	0.277
The hospital management has invested in reporting systems that capture ISM related issues	1	0.827
In this healthcare facility reporting of ISM related issues is mandatory	1	0.713
Hospital staff are alerted promptly when data softwares are undergoing upgrades in their department	1	0.602
The hospital management encourages reporting of ISM related issues	1	0.707
In this healthcare facility there is a targeted patient safety incident report procedure for ISM related issues	1	0.671
In this healthcare facility hospital management uses the reported cases to make evidence based decisions	1	0.711

Based on these Exploratory Factor Analysis results, the statement regarding the hospital's investment in reporting systems to capture ISM-related issues showed the highest extraction value at 0.827, suggesting that robust reporting infrastructure is crucial for enhancing patient safety by identifying and mitigating ISM-related risks. Similarly, the mandatory nature of reporting ISM issues demonstrated a strong communal value of 0.713, indicating its role in ensuring comprehensive documentation of potential risks. Prompt alerts for software upgrades within departments also showed a significant communal value of 0.602, indicating the importance of keeping healthcare staff informed of system changes to prevent potential disruptions to patient safety. In contrast, the relatively lower extraction value of 0.277 for the provision of a conducive reporting environment suggests that despite the fact that this factor supports patient safety, it has a less direct impact compared to more structured reporting systems. The findings indicate that dedicated, well-supported reporting systems, alongside mandatory reporting policies, are central to reducing medical errors and promoting patient

safety, while softer elements like environmental support, although beneficial, may play a secondary role in this context.

Table 4.15: Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.508	64.399	64.399	4.508	64.399	64.399
2	0.924	13.195	77.593			
3	0.488	6.972	84.566			
4	0.368	5.257	89.823			
5	0.294	4.199	94.022			
6	0.236	3.366	97.388			
7	0.183	2.612	100			

Extraction Method: Principal Component Analysis.

Table 4.15 shows that a single main factor extracted through Principal Component Analysis accounts for approximately 64.40% of the total variance in the patient safety reporting system components, with an initial eigenvalue of 4.508. This percentage of variance explained by the first factor suggests a strong and cohesive structure for the primary reporting systems influencing patient safety within the healthcare facility. Although additional components were identified, none significantly contributed to the cumulative variance, with the second component explaining only 13.20% and the remaining components each contributing less than 7%. This one-factor model indicates a dominant dimension, indicating that a unified, well-supported reporting system effectively influence the essential elements of a patient safety reporting structure within Information Security Metrics, providing a good framework for reducing medical errors and enhancing patient safety in this setting.

Table 4.16: Rotated Factor Matrix

Statement	Factor 1
In this hospital, healthcare workers are provided with conducive environment for reporting ISM incidences that affect patient safety	0.526
The hospital management has invested in reporting systems that capture ISM related issues	0.909
In this healthcare facility reporting of ISM related issues is mandatory	0.844
Hospital staff are alerted promptly when data softwares are undergoing upgrades in their department	0.776
The hospital management encourages reporting of ISM related issues	0.841
In this healthcare facility there is a targeted patient safety incident report procedure for ISM related issues	0.819
In this healthcare facility hospital management uses the reported cases to make evidence based decisions	0.843

The Rotated Factor Matrix, presented in Table 4.16, demonstrates a clear factor structure, allowing for the interpretation of Factor 1. After Varimax rotation, Factor 1 primarily captures items related to patient safety reporting systems that enhance Information Security Metrics. High loadings on statements such as the hospital's investment in reporting systems (0.909), mandatory reporting of ISM issues (0.844), management encouragement of reporting (0.841), and targeted incident reporting procedures (0.819) indicates the critical role of structured reporting systems in promoting patient safety. Additionally, prompt alerts for software upgrades (0.776) and the use of reported cases for evidence-based decision-making (0.843) emphasize the operational measures supporting effective reporting. In contrast, the lower loading on providing a conducive reporting environment (0.526) suggests that while environmental support is beneficial, it may have less direct impact compared to structured systems. This factor represents a unified framework for fostering effective ISM-related reporting processes to mitigate risks and reduce medical errors.

Discussion of EFA Findings and Descriptive Analysis Linkage

The EFA findings are consistent with the descriptive statistics, identifying a central theme within patient safety reporting systems focused on structured and operational measures to enhance Information Security Metrics (ISM). Factor 1 primarily captures structured reporting systems, as evidenced by high loadings on items such as "investment in reporting systems" (loading = 0.909), "mandatory reporting of ISM issues" (loading = 0.844), and "management encouragement of reporting" (loading = 0.841). These findings agrees with the descriptive statistics, which revealed that most of the respondents disagreed with the presence of such systems, reflected in low mean scores (e.g., mean = 2.62 for investment in reporting systems). This indicates a perceived gap in system infrastructure and management support, which is critical for effective reporting.

The lower loading for "conducive reporting environment" (loading = 0.526) in EFA corresponds with the descriptive statistics, where a majority of respondents disagreed (42.5%, mean = 3.00, SD = 1.14) on the adequacy of such an environment. Similarly, the descriptive analysis indicated mixed responses to prompt software upgrade alerts (mean = 3.09), consistent with a moderate loading of 0.776 in the factor matrix. These findings emphasize that while foundational systems and management-driven initiatives play a dominant role in fostering effective ISM reporting, softer elements like environmental support may have a less direct but still significant impact.

In synthesizing both the descriptive and EFA results, an understanding of the reporting systems emerges. The descriptive statistics highlight gaps in system implementation and perceptions of support, while the EFA consolidates these into a factor centered on structured reporting systems. This linkage suggests that addressing gaps in investment, enforcement of reporting policies, and management support is likely to improve the reporting culture and reduce medical errors, thereby promoting patient safety within the healthcare facility.

4.7 Legal Challenges of Using Information Security Metrics

The fourth objective of the study was to analyse the legal challenges of using Information Security Metrics to promote patient safety with reference to the Kenyan Data Protection Act, No. 24 of 2019. This section discusses descriptive statistics, correlation analysis and regression analysis.

4.7.1 Descriptive Statistics

The respondents were asked to indicate their levels of agreements with statements concerning the legal challenges of using information security metrics to promote patient safety in reference to the Kenyan Data Protection Act, No. 24 of 2019. The study used a scale of 1-5 such that 1-strongly disagree, 2-disagree, 3-neutral, 4-agree, 5-strongly agree. Table 4.17 shows the descriptive statistics results.

Table 4.17: Descriptive Statistics on Legal Challenges of Using ISM

Statement	Strongly disagree	Disagree	Neutral	Agreed	Strongly Agreed	Mean	Std. Dev.
In this hospital, patient engagement and approval in data collection is granted beforehand.	3.10%	20.00%	31.90%	36.90%	8.10%	3.27	0.98
In this healthcare facility patients are actively engaged in the data collection process	1.20%	17.40%	35.40%	34.20%	11.80%	3.38	0.95
In this hospital patient data privacy and confidentiality is prioritized	1.90%	13.70%	19.90%	41.60%	23.00%	3.7	1.03
In this hospital there are data policies that protect the confidentiality, availability and integrity of patient data	1.90%	13.00%	21.70%	42.90%	20.50%	3.67	1.00
In this hospital there are legal im-	1.90%	17.40%	21.10%	39.10%	20.50%	3.59	1.06

plications for sharing/altering of patient information without consent	
Overall Mean	**3.522**

The results in Table 4.17 provide opinions of the respondents' perceptions of the legal challenges of using Information Security Metrics (ISM) to promote patient safety, particularly in the context of the Kenyan Data Protection Act, No. 24 of 2019. For the statement on whether patient engagement and approval in data collection are granted beforehand, majority of respondents agreed (45%), with a mean of 3.27 and a standard deviation of 0.98. This suggests that a significant portion of participants acknowledged that consent is sought prior to data collection, although a notable percentage remained neutral, indicating some variability in the perceived practices. When asked if patients are actively engaged in the data collection process, the majority also agreed (46%, mean = 3.38, SD = 0.95). However, the high proportion of neutral responses (35.4%) suggests some uncertainty or lack of clarity about the extent of patient involvement during data collection in healthcare facilities.

A stronger consensus was observed regarding the prioritization of patient data privacy and confidentiality, with 64.6% of respondents agreeing (mean = 3.7, SD = 1.03). This high level of agreement underscores the emphasis on protecting patient information, aligning with the legal requirements set forth by the Data Protection Act. Similarly, a majority of respondents (63.4%) agreed that there are policies in place to protect the confidentiality, availability, and integrity of patient data (mean = 3.67, SD = 1.00). This finding suggests that most healthcare facilities have implemented formal data protection policies that align with the Act, contributing to secure handling of patient data.

Lastly, the majority agreed that there are legal implications for sharing or altering patient information without consent (59.6%, mean = 3.59, SD = 1.06). This agreement indicates that

most respondents are aware of the potential legal consequences of data breaches or unauthorized changes to patient information, highlighting the importance of legal compliance in information security practices. The overall mean score of 3.522 suggests that, on average, respondents positively perceive the legal and procedural measures in place to promote patient safety through ISM. However, the neutral responses in several statements indicate opportunities for further improvement of patient engagement and clarifying data protection processes in healthcare settings, ensuring full adherence to the Kenyan Data Protection Act and improving the effectiveness of ISM in safeguarding patient data.

Finally, the respondents were asked to indicate how they would rate the overall patient safety in their respective hospitals and their responses were as shown in Figure 4.6.

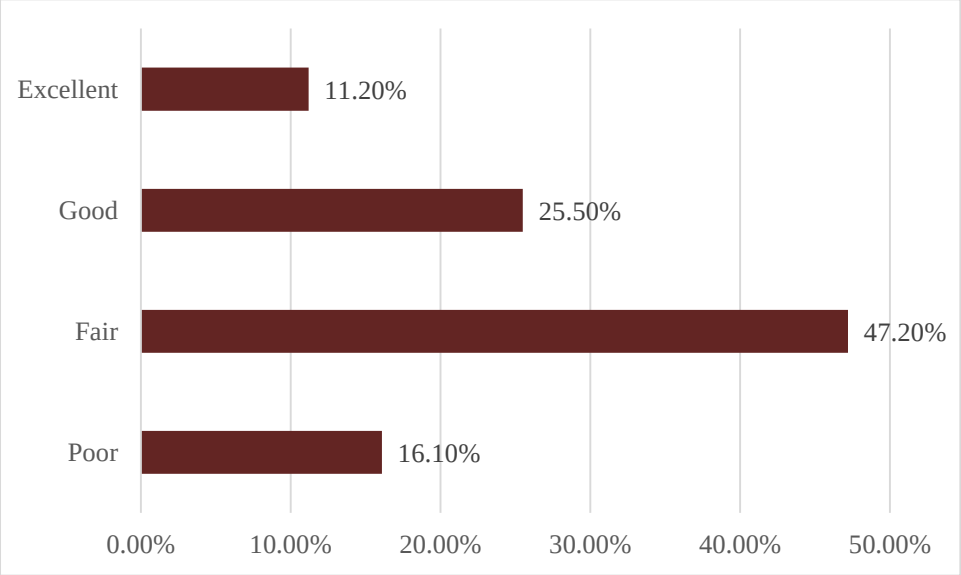


Figure 4.6: Rating the Overall Patient Safety

The results presented in the table indicate that nearly half of the respondents (47.2%) rated the overall patient safety in their respective hospitals as "Fair." A quarter of them also rated it as "Good" (25.5%), while 16.1% rated patient safety as "Poor." Only 11.2% of respondents perceived the patient safety as "Excellent." These ratings suggest that while most respondents feel that patient safety is at least adequate (Fair to Excellent), a considerable proportion views

it as needing improvement, as evidenced by the "Poor" and "Fair" ratings combined (63.3%). The relatively low percentage of "Excellent" ratings indicates that few respondents perceive patient safety to be at the highest standard. These findings imply a need for enhanced strategies and interventions to improve patient safety practices within hospitals, as well as the possibility of addressing gaps in safety measures to raise the overall perception of safety from "Fair" to "Good" or "Excellent."

4.7.2 The Exploratory Factor Analysis

The fourth objective of this study was to find out the legal challenges of using Information Security Metrics to promote patient safety in reference to the Kenyan Data Protection Act, No. 24 of 2019. Exploratory Factor Analysis was conducted using Principal Axis Factoring with Varimax rotation, and the extraction results are shown in tables 4.18. 4.19 and 4.20.

Table 4.18: Communalities

Statement	Initial	Extraction
In this hospital, patient engagement and approval in data collection is granted beforehand.	1	0.634
In this healthcare facility patients are actively engaged in the data collection process	1	0.655
In this hospital patient data privacy and confidentiality is prioritized	1	0.872
In this hospital there are data policies that protect the confidentiality, availability and integrity of patient data	1	0.841
In this hospital there are legal implications for sharing/altering of patient information without consent	1	0.896

The results of the Exploratory Factor Analysis, conducted to identify legal challenges associated with using Information Security Metrics to promote patient safety under the Kenyan Data Protection Act, No. 24 of 2019, revealed varied levels of communalities across the assessed statements. The highest extraction value (0.896) was associated with the presence of legal implications for sharing or altering patient information without consent, emphasizing the

critical role of legal enforcement in safeguarding patient data. Similarly, the prioritization of patient data privacy and confidentiality showed a strong communal value of 0.872, highlighting its importance in complying with data protection laws and promoting trust in healthcare services.

Additionally, data policies protecting confidentiality, availability, and integrity of patient data also demonstrated a high extraction value of 0.841, suggesting that well-defined policies are fundamental to addressing legal challenges in Information Security Metrics. Patient engagement in the data collection process showed moderate extraction values (0.634 and 0.655), indicating that while engagement practices support legal compliance, they may have a less direct impact compared to enforcement mechanisms and data policies. These findings indicates the necessity of strong legal frameworks and policies, alongside active patient engagement, to mitigate legal challenges and enhance patient safety.

Table 4.19: Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumula-tive %	Total	% of Variance	Cumula-tive %
1	3.899	77.975	77.975	3.899	77.975	77.975
2	0.467	9.34	87.315			
3	0.408	8.165	95.48			
4	0.152	3.04	98.519			
5	0.074	1.481	100			

Extraction Method: Principal Component Analysis.

Table 4.19 reveals that a single main factor extracted through Principal Component Analysis accounts for approximately 77.98% of the total variance in the legal challenges related to the use of Information Security Metrics under the Kenyan Data Protection Act, No. 24 of 2019, with an initial eigenvalue of 3.899. This high percentage of variance explained by the first factor indicates a strong and cohesive representation of the primary legal considerations

influencing patient safety. Although additional components were identified, their contributions were negligible, with the second component explaining only 9.34% and the remaining components each contributing less than 9%. This one-factor model underscores the dominant role of legal compliance, including patient data privacy, confidentiality, and legal enforcement mechanisms, as key dimensions in mitigating challenges and promoting patient safety within the healthcare framework. The findings suggest that an effective legal structure is necessary for addressing the challenges associated with implementing Information Security Metrics effectively in healthcare settings.

Table 4.20: Rotated Factor Matrix

Statement	Factor 1
In this hospital, patient engagement and approval in data collection is granted beforehand.	0.796
In this healthcare facility patients are actively engaged in the data collection process	0.809
In this hospital patient data privacy and confidentiality is prioritized	0.934
In this hospital there are data policies that protect the confidentiality, availability and integrity of patient data	0.917
In this hospital there are legal implications for sharing/altering of patient information without consent	0.947

The Rotated Factor Matrix, presented in Table 4.20, demonstrates a clear factor structure, allowing for the interpretation of Factor 1. After Varimax rotation, Factor 1 primarily captures items related to legal compliance and data governance within Information Security Metrics. High loadings on statements such as "legal implications for sharing/altering patient information without consent" (0.947), "patient data privacy and confidentiality is prioritized" (0.934), and "data policies protecting confidentiality, availability, and integrity" (0.917) highlight the critical role of legal enforcement and structured policies in safeguarding patient data. Additionally, the engagement of patients in data collection, both through prior approval (0.796) and active involvement (0.809), emphasizes the importance of patient consent and participation in ensuring compliance with the Kenyan Data Protection Act. These findings reflect a unified

approach to legal compliance and data protection, underscoring the necessity of robust policies, enforcement mechanisms, and patient-centric practices to address legal challenges and enhance patient safety in healthcare.

Discussion of EFA Findings and Descriptive Analysis Linkage

The EFA findings are consistent with the descriptive statistics, revealing a central theme focused on legal compliance and governance in using Information Security Metrics (ISM) to promote patient safety. Factor 1 primarily captures legal compliance and structured data governance, as evidenced by high loadings on items such as "legal implications for sharing/altering patient information without consent" (loading = 0.947), "patient data privacy and confidentiality is prioritized" (loading = 0.934), and "data policies protecting confidentiality, availability, and integrity" (loading = 0.917). These findings align with the descriptive statistics, which show strong agreement among respondents that privacy and confidentiality are prioritized (mean = 3.7) and that formal data protection policies are in place (mean = 3.67). This demonstrates a high level of adherence to key aspects of the Kenyan Data Protection Act.

The lower EFA loadings for patient engagement in data collection, both for prior approval (loading = 0.796) and active involvement (loading = 0.809), correspond with the descriptive statistics where these items had relatively lower mean scores (3.27 and 3.38, respectively) and significant neutral responses. These findings suggest that while patient engagement is acknowledged, it is less robustly implemented compared to legal enforcement mechanisms and policies.

Through synthesizing both the descriptive and EFA results, a comprehensive understanding emerges of the legal challenges in ISM. The descriptive statistics highlight areas for improvement, particularly in patient engagement and clarity of data collection practices, while

the EFA consolidates these elements into a factor centered on legal frameworks and governance. This linkage suggests that while robust policies and legal enforcement are critical, addressing gaps in patient engagement and ensuring consistent implementation of practices further strengthen ISM's role in promoting patient safety and compliance with the Kenyan Data Protection Act. These findings show that the problem actually was existent in hospitals in Nairobi.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents summary of key findings as discussed in the previsions chapter. The chapter also presents conclusions drawn from the findings after which recommendations are presented in view of the study findings. The chapter concludes by presenting suggestions for further studies.

5.2 Summary of Findings

The purpose of this study was to find out what challenges are experienced in the use of Information Security Metrics to improve patient safety at public referral hospitals in Nairobi Metropolitan. Specifically, the study sought to; find out which technical components of Information Security Metrics are in place and their effects in promoting patient safety, identify security controls that protects the Privacy, Integrity and Accessibility of data in Information Security Metrics in promoting patient safety, identify key patient safety reporting systems in Information Security Metrics that help in reducing medical errors and find out the legal challenges of using Information Security Metrics to promote patient safety in reference to the Kenyan Data Protection Act, No. 24 of 2019. The summary of key findings are presented below per study objective.

5.2.1 Technical Components and Patient Safety

The study sought to find out which technical components of Information Security Metrics are in place and their effects in promoting patient safety. The study found that the technical components of Information Security Metrics (ISM) in healthcare facilities play a role in promoting patient safety. Respondents largely agreed that their healthcare facilities have data collection software in place for managing patient data (57.2%, Mean = 3.46, SD = 1.03), and

most acknowledged that backup generators are available to support the storage of patient information during power outages (69.9%, Mean = 3.83, SD = 0.86). However, the study also identified key challenges, including the perception that healthcare staff are inadequately trained in the use of ISM (48.7% disagreed, Mean = 2.76, SD = 1.22) and the lack of immediate technical support for resolving ISM issues (50.5% disagreed, Mean = 2.92, SD = 1.33). The overall mean score of 3.057 suggested that while some technical components were in place, improvements are necessary to enhance the use and impact of ISM in patient safety.

The Exploratory Factor Analysis (EFA) identified two primary factors within Information Security Metrics (ISM) components: management and organizational commitment, and infrastructure and technical support. Factor 1, representing management and organizational commitment, accounted for 40.18% of the variance and included high loadings for items such as "hospital management prioritizes ISM" (loading = 0.911) and "culture of evidence-based decision-making" (loading = 0.793). These findings emphasized the critical influence of a supportive management structure in fostering effective ISM practices. The descriptive statistics corroborated this, highlighting moderate engagement from management, with gaps in leadership commitment potentially hindering ISM's integration into patient safety practices.

Factor 2, representing infrastructure and technical support, explained an additional 23.89% of the variance and included components such as "availability of devices" (loading = 0.715), "backup generators" (loading = 0.478), and "standby technicians for ISM issues" (loading = 0.767). Descriptive findings revealed that while some infrastructural elements like device availability were relatively well-supported, other areas, including prompt technical issue resolution, scored lower. Together, these findings indicated that while foundational infrastructure and management structures are in place, gaps remain in organizational support and responsiveness, which are crucial for ISM's effectiveness in enhancing patient safety.

Addressing these areas could significantly improve ISM's role in safeguarding patient data and ensuring safety within healthcare facilities.

5.2.2 Security Controls and Patient Safety

The second objective of the study was to identify security controls that protects the Privacy, Integrity and Accessibility of data in Information Security Metrics in promoting patient safety. The study found that security controls protecting the privacy, integrity, and accessibility of data are integral to promoting patient safety in healthcare facilities. A significant number of respondents acknowledged the importance of certain security controls, such as system access mechanisms, with 67% agreeing that proper controls like user accounts were in place (Mean = 3.96, SD = 0.69). Additionally, 45.9% of respondents agreed that patient data was adequately protected from illegal access and accidental loss (Mean = 3.73, SD = 0.94), suggesting confidence in existing security measures. However, there were areas of concern, such as a lower agreement on the acceptability of sharing computer passwords (35.9% disagreed, Mean = 2.85, SD = 1.33), indicating awareness of potential risks but also suggesting variability in security practices across facilities.

The study identified key security controls protecting the privacy, integrity, and accessibility of data within Information Security Metrics through Exploratory Factor Analysis (EFA). The results showed that firewall-enabled computers (extraction value = 0.697) and up-to-date antivirus software (0.720) were critical in safeguarding patient data, while security controls preventing theft and hacking had the highest extraction value (0.825), emphasizing their role in ensuring data confidentiality. In contrast, system access control mechanisms, such as user accounts, demonstrated a lower extraction value (0.290), suggesting that while they contributed to overall security, they were less impactful than technical controls. These findings highlighted the prominence of tangible protections like firewalls and antivirus software in promoting patient safety while pointing to the need for enhanced procedural controls.

The EFA results revealed that a single factor explained 60.09% of the total variance in security controls, indicating a cohesive representation of the primary measures influencing patient safety. High factor loadings for items such as "firewall-enabled computers" (0.835) and "up-to-date antivirus software" (0.849) reinforced the facility's reliance on technical measures to protect patient data. However, password-sharing practices showed a negative loading (-0.582), reflecting their detrimental impact on data security. These findings suggested that while technical security controls were effective, procedural practices, such as consistent access controls, needed improvement. Overall, the study emphasized the importance of strengthening both technical and procedural security measures to enhance patient safety in healthcare settings.

5.2.3 Key Patient Safety Reporting Systems and Patient Safety

The third objective was to identify key patient safety reporting systems in Information Security Metrics that help in reducing medical errors. The study found that key patient safety reporting systems in information security metrics (ISM) are crucial in reducing medical errors and promoting patient safety. A significant portion of respondents perceived gaps in supportive environments for reporting ISM incidents, with 42.5% disagreeing that healthcare workers are provided with a conducive environment (Mean = 3.00, SD = 1.14). Moreover, 50.9% of respondents disagreed that hospital management invested adequately in systems for reporting ISM-related issues (Mean = 2.62, SD = 1.1), suggesting a perceived lack of sufficient infrastructure for incident reporting. A lack of enforced protocols was also noted, with 48.5% of respondents disagreeing that reporting ISM issues is mandatory (Mean = 2.72, SD = 0.99). These findings highlight challenges in fostering an open reporting culture, establishing robust reporting systems, and ensuring mandatory reporting procedures.

The Exploratory Factor Analysis (EFA) results revealed that the hospital's investment in reporting systems to capture ISM-related issues had the highest extraction value (0.827), highlighting the importance of robust reporting infrastructure in mitigating ISM-related risks.

Similarly, mandatory reporting of ISM issues (extraction value = 0.713) and prompt alerts for software upgrades (0.602) were shown to play critical roles in ensuring comprehensive risk documentation and maintaining uninterrupted patient safety processes. However, the relatively low extraction value for providing a conducive reporting environment (0.277) suggested that while environmental support contributes to patient safety, it has a lesser impact compared to structured systems and mandatory reporting policies.

The EFA results showed that a single factor accounted for 64.40% of the variance in patient safety reporting systems, indicating a strong and unified framework for ISM-related reporting processes. The Rotated Factor Matrix highlighted the importance of structured systems, with high loadings on items such as "investment in reporting systems" (0.909), "mandatory reporting of ISM issues" (0.844), and "management encouragement of reporting" (0.841). These findings were consistent with the descriptive statistics, which revealed low mean scores (e.g., mean = 2.62 for investment in reporting systems), indicating gaps in system infrastructure and management support. The low loading for a conducive reporting environment (0.526) corresponded with the descriptive finding that 42.5% of respondents disagreed with its adequacy (mean = 3.00, SD = 1.14). Together, the results underscored the need to strengthen reporting infrastructure, enforce reporting policies, and enhance management support to foster an effective reporting culture, reduce medical errors, and improve patient safety in healthcare facilities.

5.2.4 Legal Challenges and Patient Safety

The fourth objective sough to find out the legal challenges of using Information Security Metrics to promote patient safety in reference to the Kenyan Data Protection Act, No. 24 of 2019. The study found that legal challenges associated with using Information Security Metrics (ISM) significantly impact patient safety, particularly in the context of the Kenyan Data Protection Act, No. 24 of 2019. The descriptive statistics revealed varied perceptions among

respondents regarding these legal challenges. For instance, 45% of respondents agreed that patient engagement and approval in data collection are sought beforehand (Mean = 3.27, SD = 0.98), indicating a positive acknowledgment of consent practices. However, a substantial proportion remained neutral, suggesting variability in perceived practices regarding patient involvement in data collection. Additionally, 46% of respondents agreed that patients are actively engaged in the data collection process (Mean = 3.38, SD = 0.95), although the high neutral response indicates uncertainty about the level of engagement.

A significant consensus was observed regarding the prioritization of patient data privacy and confidentiality, with 64.6% agreeing that these aspects are emphasized (Mean = 3.7, SD = 1.03). This aligns with the legal requirements outlined in the Data Protection Act, reflecting a general commitment to safeguarding patient information. Moreover, 63.4% agreed that policies exist to protect the confidentiality, availability, and integrity of patient data (Mean = 3.67, SD = 1.00), suggesting that many healthcare facilities have implemented measures to comply with legal standards. Additionally, 59.6% acknowledged the legal implications of sharing or altering patient information without consent (Mean = 3.59, SD = 1.06), highlighting awareness of the potential legal consequences of data breaches.

The Exploratory Factor Analysis (EFA) results revealed that legal implications for sharing or altering patient information without consent had the highest extraction value (0.896), highlighting the importance of strict enforcement mechanisms in protecting patient data. Similarly, the prioritization of patient data privacy and confidentiality (0.872) and the presence of data policies protecting confidentiality, availability, and integrity (0.841) demonstrated strong communal values, underscoring their role as foundational components of legal compliance. In contrast, patient engagement in the data collection process, both through prior approval (0.634) and active involvement (0.655), showed moderate extraction values,

suggesting a supportive but less direct impact compared to legal enforcement and structured policies.

The EFA findings indicated that a single factor accounted for 77.98% of the total variance in legal challenges, with high loadings on items such as "legal implications for sharing/altering patient information without consent" (0.947), "patient data privacy and confidentiality is prioritized" (0.934), and "data policies protecting confidentiality, availability, and integrity" (0.917). These findings were consistent with the descriptive statistics, which showed strong agreement among respondents that legal frameworks and policies were in place (mean = 3.67 for data protection policies) and that privacy and confidentiality were prioritized (mean = 3.7). However, patient engagement, reflected in lower factor loadings (0.796 for prior approval and 0.809 for active involvement), aligned with moderate descriptive statistics (mean = 3.27 and 3.38, respectively), indicating that engagement practices were less robustly implemented. Together, the findings emphasized the importance of strengthening patient engagement and maintaining robust legal frameworks to address challenges effectively and enhance patient safety in compliance with the Kenyan Data Protection Act.

5.3 Conclusion

The study concludes that effective implementation of Information Security Metrics (ISM) is necessary for enhancing patient safety in healthcare facilities. It highlights the significant role that both technical components and security controls play in safeguarding patient data while promoting a safe healthcare environment. Additionally, the findings indicate the necessity of addressing legal challenges that can hinder the effective use of ISM, particularly in compliance with the Kenyan Data Protection Act, No. 24 of 2019. This multifaceted approach emphasizes that improving patient safety requires a holistic understanding of the interrelated factors affecting ISM practices.

Furthermore, the positive correlations found between the technical components of ISM and patient safety indicate that improvements in information security measures can lead to better safety outcomes. The study demonstrates that the availability of adequate technical resources, such as data collection software and backup systems, is foundational for protecting patient information and reducing medical errors. However, the identified gaps in staff training and immediate technical support reveal that organizations must invest more in developing the competencies of healthcare workers to effectively utilize these systems.

The findings regarding security controls further confirm their integral role in promoting patient safety. The results indicate that robust security measures, including proper access controls and data protection policies, are essential in mitigating risks related to data breaches and unauthorized access. The study highlights the need for healthcare facilities to prioritize the establishment and maintenance of these controls to enhance patient safety and build trust with patients concerning their data privacy.

Moreover, the analysis of legal challenges provides valuable insights into the barriers that healthcare organizations face when implementing ISM. The strong negative correlation between legal challenges and patient safety indicates that difficulties in adhering to legal requirements can significantly impair patient safety outcomes. This indicates the importance of addressing these legal hurdles to create an environment that fosters effective reporting systems and a culture of safety.

The study emphasizes that enhancing patient safety requires a comprehensive approach that encompasses technical improvements, robust security controls, and effective navigation of legal challenges. By addressing these interconnected factors, healthcare facilities can improve their information security practices, ultimately leading to better patient safety outcomes. The results advocate for increased investment in staff training, infrastructure, and compliance

measures to ensure that patient safety is prioritized and upheld in accordance with legal standards.

5.4 Recommendations for Policy Application

Based on the findings of the study, several recommendations for policy application can be made to enhance the effectiveness of Information Security Metrics (ISM) in promoting patient safety within healthcare facilities. The study recommends that hospitals should consider prioritizing the development and implementation of comprehensive training programs for staff on the use of ISM tools and protocols. Given that a significant portion of respondents indicated inadequate training, policies should mandate regular training sessions that not only cover the technical aspects of ISM but also emphasize the importance of data security in patient safety. Through equipping staff with the necessary skills and knowledge, these hospitals are able to create a more informed workforce that is capable of effectively managing patient data and responding to incidents promptly.

Additionally, healthcare facilities should invest in improving the technical infrastructure that supports ISM practices. The study discusses gaps in the availability of essential technical components, such as adequate computers and user-friendly data collection software. Policies should encourage budget allocations specifically aimed at upgrading technological resources and ensuring that they are accessible to all staff members involved in patient care. Additionally, the establishment of a centralized IT support system could be beneficial in providing immediate assistance for any technical issues that arise, thereby minimizing disruptions in patient care.

In light of the positive relationship found between security controls and patient safety, it is imperative for healthcare organizations to develop and enforce stringent security policies. This includes the implementation of robust access control mechanisms, regular updates of antivirus software, and ensuring that firewalls are in place to protect sensitive patient data. Policies

should stipulate that all healthcare workers receive training on the importance of these security measures, as well as the consequences of breaches in data security. By reinforcing a culture of security awareness, organizations can significantly reduce the risks associated with data breaches and enhance overall patient safety.

Furthermore, addressing the legal challenges as indicated in the study is essential for the effective application of ISM in promoting patient safety. Policies should be developed to ensure that healthcare organizations are fully compliant with the Kenyan Data Protection Act, No. 24 of 2019. This should involve the formation of legal advisory committees within healthcare facilities to guide management on compliance matters and establish clear protocols for handling patient data. By ensuring adherence to legal standards, organizations can protect themselves from potential legal repercussions while simultaneously improving patient trust in the handling of their sensitive information.

In addition, healthcare organizations should foster an environment that encourages open communication and reporting of ISM-related incidents. The study revealed a lack of support for reporting safety incidents, which can hinder the identification of issues that affect patient safety. Policies should be implemented to create a non-punitive reporting culture that encourages healthcare workers to report incidents without fear of retribution. This could include anonymous reporting systems and regular feedback sessions where staff can discuss challenges and suggest improvements to existing ISM practices.

Lastly, hospitals should strive to engage in continuous evaluation and improvement of their ISM practices. Policies should mandate regular audits and assessments of ISM systems to identify areas for improvement and ensure that they remain effective in promoting patient safety. These evaluations should involve gathering feedback from staff on the usability and effectiveness of ISM tools and incorporating this feedback into the ongoing development of

security protocols. These hospitals should be able to adapt to evolving challenges and enhance their capacity to protect patient data and promote safety in healthcare settings.

5.5 Recommendation for Further Research

- This study aimed at exploring the contributions of Information Security Metrics (ISM) to patient safety within healthcare facilities, specifically focusing on technical components, security controls, patient safety reporting systems, and legal challenges. Future research should consider the impact of organizational culture, leadership styles, and employee engagement on the effectiveness of ISM in promoting patient safety. These variables could provide a more comprehensive understanding of the factors influencing ISM implementation and its outcomes on patient safety.
- Future studies should expand beyond healthcare staff perceptions to include insights from a broader range of stakeholders, such as patients, IT professionals, and healthcare administrators. This multi-stakeholder approach can enhance the findings and offer a more diverse view on the effectiveness of ISM practices. Qualitative methods, like interviews or focus groups, should be incorporated to provide deeper context and uncover underlying issues affecting ISM and patient safety.
- To provide a comparative analysis, future research should replicate this study across different healthcare facilities, regions, or countries. Such expansions could identify contextual differences and offer a broader understanding of how various factors influence the implementation of ISM and its impact on patient safety.

REFRENCES

Abbas, R., Pitt, J., & Michael, K. (2021). Socio- Technical Design for Public Interest Technology . *IEEE* .

Ajwang', B., Komen, A., & Ngaira, D. &. (2019). *Enhancing health information system for evidence based decision making in the health sector.* Nairobi: MOH,Kenya.

AlHogail, A. (2015). Design and validation of information security culture framework. . *Computers in human behaviour* , 49,567-575.

Alotaibi, Y. K., & Federico, F. (2017). The impact of health information technology on patient safety. *Saudi Med J* .

Amin, A., Lairumbi, G., & Watson-Grant, S. (2015). *MEASURE Evaluation* .

Andres, J. (2014). *The basics of information security.* Boston.

Astier, A., Carlet, J., & Hoppe-Tichy, T. (2020). What is the role of technology in improving patient safety? A French, German and UK healthcare professional perspective. *Journal of Patient Safety and Risk Management* .

Bas, S. (2015). *Developing conceptual framework for research.*

Bednar, P., & Welch, C. (2020). Socio-Technical Perspective on Smart working: Creating Meaningful and Sustainable Systems. *Informations Systems Frontiers* .

Benet, R. (2017). Avoiding philosophy as a trump-card in sociological writing. A study from the discourse of evidence-based healthcare. *Social Theory & Health* .

Berwick, D. (2013). A promise to learn-a commitment to act:improving the safety of patients in England. page 27.

Burisch, R., & Wohlgemuth, V. (2016). Blind spots of dynamic capabilities: A systems theoretic perspective. *Journal of Innovation and Knowledge* .

Cabric, M. (2015). *Corporate security management: confidentiality, integrity, availability.*

Chang, V., & Ramachandran, M. (2015). *Towars achieving data security with the cloud computing adoption framework.* IEEE Transactions on Services Computing.

Charlotte, A., Marion, J., George, R., & Joan, M. (2016). *Health Information Management Systems.* Springer.

Cohen, L., Morrison, L., & Manion, L. (2018). *Research Methods in Education (8th ed.).* London: Routledge.

Cooper, V., & Molla, A. (2017). Information systems absorptive capacity for environmentally driven IS-enabled transformation. *Information Systems Journal* .

Dave, B., & David, T. B. (2019). Information Systems for Business and Beyond. *Information Systems Security Journal* .

Dilli, S., Simon, E. Y., Jin-Hee, C., Terrence, M. J., & Nelson, F. (2020). Dynamic Security Metrics for Software-Defined Network-Based Moving Target Defense. *Journal of Network and Computer Applications* .

Emery, F. E. (2016). Characteristics of Socio- Technical Systems. *The Social Engagement of Social Science* .

Faozi, A., Najib, H. S., Ali, Y. T., Borhan, O. A., & Mohd, S. (2022). The mediating effect of IT governance between coporate governance mechanisms, business continuity, and transparency and disclosure: An empirical study of COVID-19 Pandemic in Jordan. *Information Security Journal: A Global Perspective* .

Janusz, Z., Steven, D., William, M., & Andrew, J. K. (2018). Measuring Security: A Challenge for the Generation. *Federated Conference on Computer Science and Information Systems.*

Jenkins, D., Sharfeen, R. Q., Moinudheen, J., Pathan, S. A., & Thomas, S. (2020). Evaluation of Electronic Medical Record Downtime in a busy Emergency Department. *Qatar Med J.*

Julia, G. (2018). Observational Studies and their Utility for Practice. *Aust. Prescr.* , 82-85.

Kapoor, K., Ziaee, A. B., Dwivedi, Y. K., Schroeder, A., Beltagui, A., & Baines, T. (2021). A socio-technical view of platform eco sysytems: Systematic review and research agenda. *Journal of business research* .

Katuu, S. (2016). Transforming South Africa's health sector: the ehealth strategy, the implementation of electronic document and records management system and the utility of maturity models. *Journal of science and technology policy management* , 330-345.

Kean, B., & Cochrane, D. T. (2021). Data as asset? The measurement, goverance and valuation of digital personal data by Big Tech. *Big Data & Society* .

Klaus, H., Susanne, B., & Martyn, P. (2019). Datafication and accountability in public health: Introduction to a special issue. *Social Studies of Science* .

KNBS. (2019). *National Census.*

KNH. (2018). *KNH strategic plan 2018-2023.* Nairobi.

Larsen, E., Fong, A., Wernz, C., & Ratwani, R. (2018). Implications of electronic health record downtime: an analysis of patient safety event reports. *J Am Med Inform Assoc* .

Linda, M. H., Hannah, S. B., Allison, M. B., & Heather, A. H. (2017). Electronic Health Records and the Disappearing patient. *Medical Anthropology Quarterly* .

Liu, J. (2022). Social Data Governance: Towards a definition and model. *Big Data & Society* .

Makary, M. A., & Daniel, M. (2016). *Medical Error-the third leading cause of death in the US.* BMJ.

Marlee, T., & Devi, S. (2019). Metric partnerships: global burden of disease estimates within the world bank, the World Health Organization and the institute for Health Metrics and Evaluation. *Wellcome Open Research* .

Martin, G., Ali, K., Steve, E., & Paulo, S. (2018). the Theoretical foundations of sociotechnical systems change for sustainability. *Journal of Cleaner Production* .

Maxfield, G., & Babbie, R. (2017). *Research Methods for Criminal Justice and Criminology 8th Ed.* Cengage Learning.

Ahouanmenou, S., Van Looy, A., & Poels, G. (2023). Information security and privacy in hospitals: a literature mapping and review of research gaps. *Informatics for Health and Social Care*, *48*(1), 30-46.

Alsahli, S. S., Almalki, M. H. M., Alkhathami, A. M., Alharbi, A. A., Alhawit, M. E., Albalawi, K. I., ... & Binselm, K. R. A.(2024). Quality Improvement and Patient Safety: Strategies

and Challenges in Healthcare System Transformation. *International journal of health sciences*, *4*(S1), 478-497.

Neri, M., Benevento, E., Stefanini, A., Aloini, D., Niccolini, F., Carducci, A., ... & Dini, G. (2024). Understanding information security awareness: evidence from the public healthcare sector. *Information & Computer Security*.

Andersen Nigeria. (2023). *Cybersecurity Risks in Healthcare: Addressing Africa's Digital Health Vulnerabilities*. Retrieved from https://ng.andersen.com/cybersecurity-risks-in-healthcare-addressing-africas-digital-health-vulnerabilities/

Bagyendera, M., Nabende, P., Godman, B., & Nabukenya, J. (2024). *Contextualizing Syntactic Interoperability Data Standards for Health Information Exchange in Uganda's Public Healthcare System*. Retrieved from https://www.scitepress.org/Papers/2024/127111/127111.pdf

Chuma, K. G. (2019). *Security of Electronic Personal Health Information in a Public Hospital in South Africa*. University of South Africa. Retrieved from https://uir.unisa.ac.za/bitstream/10500/27239/1/dissertation_chuma_kg.pdf

Serianu. (2020). *Africa Cybersecurity Report - Uganda 2019/2020*. Retrieved from https://www.serianu.com/downloads/UgandaCyberSecurityReport2020.pdf

Waddell, M. (2024, January). Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. In *Healthcare Management Forum* (Vol. 37, No. 1, pp. 13-16). Sage CA: Los Angeles, CA: SAGE Publications.

Ayugi, E. (2021). *Information Security Strategies and Patient Data Privacy Among Health Facilities in Nairobi*. University of Nairobi. Retrieved from https://erepository.uonbi.ac.ke/bitstream/handle/11295/157072/Ayugi%20E_Information%20Security%20Strategies%20and%20Patient%20Data%20Privacy%20Among%20Health%20Facilities%20in%20Nairobi.pdf?sequence=1

Okutoyi, L., Godia, P., Adam, M., Sitati, F., & Jaoko, W. (2024). *Understanding Diagnostic Error Patterns and Contributing Factors: A Descriptive Analysis of Medical Error Reports at a Tertiary Hospital in Kenya 2019-2021*. medRxiv. Retrieved from https://www.medrxiv.org/content/10.1101/2024.05.21.24307687v1.full.pdf

Okutoyi, L., Godia, P., Adam, M., Sitati, F., & Jaoko, W. (2022). *Medical Error Reporting Among Healthcare Workers in a Kenyan Tertiary Level Hospital: A KAP Study*. ResearchGate. Retrieved from https://www.researchgate.net/publication/374314295_Medical_Error_Reporting_Among_Healthcare_Workers_in_a_Kenyan_Tertiary_Level_Hospital_A_KAP_Study

World Bank Group. (2022). *An Assessment of Patient Safety Standards in Kenya*. Retrieved from https://uasingishureproductivehealth.files.wordpress.com/2015/08/kenya-patient-safety-survey-report-2014.pdf

Menard, P., Bott, G. .., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self determination theory. *Journal of Management Information Systems* .

Adeyemi, C., Adegoke, B. O., & Odugbose, T. (2024). The impact of healthcare information technology on reducing medication errors: A review of recent advances. *International journal of frontiers in medicine and surgery research[online]*, *5*(2), 20-29.

Olusanya, M., & Peter, E. (2024). Analysis of the Impact of Digitalisation of Healthcare Service: An Emphasis on the Digitalisation of ClinicsAcross Nigeria.

Mujuni, D., Tumwine, J., Musisi, K., Otim, E., Farhat, M. R., Nabulobi, D., ... & Joloba, M. (2024). Beyond diagnostic connectivity: Leveraging digital health technology for the real-time collection and provision of high-quality actionable data on infectious diseases in Uganda. *PLOS Digital Health*, *3*(8), e0000566.

Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. *International nursing review*, *67*(2), 218-230.

Jawad, L. A. (2024). Security and privacy in digital healthcare systems: Challenges and mitigation strategies. *Abhigyan*, *42*(1), 23-31.

Hamapa, A. M., Zulu, J. M., Khondowe, O., & Hangulu, L. (2024). Healthcare workers' perceptions and user experiences of biometric technology in the selected healthcare facilities in Zambia. *Discover Public Health*, *21*(1), 47.

Kimathi, M. E. (2024). An Assessment Of Cloud Computing And Its Impact On Data Security In Healthcare: A Case Study Of M-Tiba.

Ferrara, M., Bertozzi, G., Di Fazio, N., Aquila, I., Di Fazio, A., Maiese, A., ... & La Russa, R. (2024, February). Risk management and patient safety in the artificial intelligence era: a systematic review. In *Healthcare* (Vol. 12, No. 5, p. 549). MDPI.

Mensah, N. K., Adzakpah, G., Kissi, J., Taylor-Abdulai, H., Johnson, S. B., Agbeshie, P. A., ... & Boadu, R. O. (2024). Health Professionals' Ethical, Security, and Patient Safety Concerns Using Digital Health Technologies: A Mixed Method Research Study. *Health Services Insights*, *17*, 11786329241303379.

Nthumba, P. M., Mwangi, C., & Odhiambo, M. (2024). Patient safety in a rural sub-Saharan Africa hospital: A 7-year experience at the AIC Kijabe Hospital, Kenya. *PLOS Global Public Health*, *4*(11), e0003919.

Reddy, S. (2025). Global Harmonization of Artificial Intelligence-Enabled Software as a Medical Device Regulation: Addressing Challenges and Unifying Standards. *Mayo Clinic Proceedings: Digital Health*, *3*(1).

Solimini, R., Busardò, F. P., Gibelli, F., Sirignano, A., & Ricci, G. (2021). Ethical and Legal Challenges of Telemedicine in the Era of the COVID-19 Pandemic. *Medicina*, *57*(12), 1314.

McGivern, G., Wafula, F., Seruwagi, G., Kiefer, T., Musiega, A., Nakidde, C., ... & English, M. (2024). Deconcentrating regulation in low-and middle-income country health systems: a proposed ambidextrous solution to problems with professional regulation for doctors and nurses in Kenya and Uganda. *Human Resources for Health*, *22*(1), 13.

Dissanayake, D. A. P., Dharmasena, K. P., & Warnakulasuriya, S. S. P. (2024). Challenges of integrating patient safety into nursing curricula: An integrative literature review. *Journal of Patient Safety and Risk Management*, *29*(1), 8-35.

Michael, B., Nicolas, B., & Philipp, O. (2021). Disentangling the Concept of Information Security Properties- Enabling Effective Information Security Governance. *European Conference on Information Systems.*

MOH. (2020). *An assessment of patient safety standards in Kenya.* Nairobi.

MOH. (2018). Kenya health information systems:interprobabillity framework.

Noel, W. (2016). *An Investigation of Socio-Technical Components of Knowledge Manangement System Usage.* Florida: NSU.

O'Brien, N., Ghafur, S., & Durkin, M. (2021). *Cybersecurity in health is an urgent patient safety concern: We can leran from exisiting safety improvement strategies to address it.* Journal of Patient Safety and Risk Management.

Omar, S. (2017). Information System security threats and vulnerabilities: evaluating the human factor in data protection. *Doctoral dissertation* .

Palojoki, S., Saranto, K., Reponen, E., Skants, N., Vakkuri, A., & Vuokko, R. (2021). Classification of Electronic Health Record-Related Patient Safety Incidents: Development and Validation Study. *JMIR Med Inform* .

Pitt, J., Dryzek, J., & Ober, J. (2020). Algorithmic Reflexive Governance for Socio-Techno-Ecological Systems. *IEEE* .

Ponto, J. (2015). Understanding and Evaluating Survey Research . *Journal of Advanced Practitioner in Oncology* .

Rana, K., & Abbas, A. (2017). Security Metrics and the risks: An Overview.

Sabi, H. M., Uzoka, F. M., Langmia, K., Njeh, F. N., & Tsuma, C. K. (2018). a cross-country model of contextual factors impacting cloud computing adoption at universities in Sub Saharan Africa. *Information System Frontiers* .

Santos, H., Andre, O., Lucia, S., & Alan, S. (2021). information Security Assessment and Certification within Supply Chains. *ARES 2021*.

Savaget, P., & Acero, L. (2017). *Plurality in understandings of innovation, sociotechnical progress and sustainable development.*

Schneider, E., Ridgely, M., Meeker, D., Hunter, L., Khodyakov, D., & Rudin, R. (2014). *Promoting patient safety through effective effective health information technology risk management.* RAND Health.

Soohyun, J., Insoo, S., & Han, J. (2022). Understanding employees's emotional reactions to ISSP compliance: focus on frustration from security requirements. *Behaviour and Information Technology* .

Taber, K. S. (2018). The Use of Cronbach's Alpha when Developing and Reporting Research Instruments in Science Education. *Res Sci Educ* .

Tim, R., & Kari, L. (2019). Evidence-making interventions in health: A conceptual framing. *Social Science & Medicine* .

Vincent, C. A., Burnett, S., & Carthey, C. (2013). *The measurement and monitoring of safety in healthcare.* London: Health Foundation.

Vuokko, R., Vakkuri, A., & Palojoki, S. (2022). *Preliminary Exploration of main Elements for Systematic Classification Development: Case Study of Patient Safety Incidents.*

Wambugu, S., & Villella, C. (2020). *Low- and middle- income countries: challenges and opportunities in data quality, privacy and security.* MEASURE evaluation.

Warkentin, M., Mcbride, M., Carter, L., & Johnston, A. C. (2016). Dispositional and situational factors: Influenece of information security policy violations. *European Journal of Information Systems* .

WHO. (2020). *Monitoring health for the SDGs.*

WHO. (2018). *Patient safety in developing and transitional countries.*

WHO. (2017). Patient safety:making health care safer.

Yazdanmehr, A., & Wang, J. (2016). Employee's information security policy compliance: A norm activation perspective. *Decision Support Systems* , 36-46.

Zare, H., Olsen, P., Zare, M., & Azadi, M. (2018). *Operating System Security Management and Ease of Implemantation (Passwords, firewalls and antivirus).* Springer.

APPENDICES

Appendix I: Informed Consent

My name is **Maryanne Waithera Mwaura**, a post graduate student at Kenyatta University pursuing Masters of Security Management and Police Studies. I shall be conducting a study on: The challenges of using Information Security Metrics to improve patient safety in public medical centres, in Nairobi Metropolitan, Kenya. The information you offer will only be used for academic intents and to help improve patient safety.

Procedures to be followed

Engagement in this research requires that I ask you some questions. I will document the data from you in a questionnaire.

You have the right to refuse to participate in this project. Kindly remember that involvement in this research is voluntary. You may ask questions relating to the project at any time. You may decline answering any queries and halt the interview at any time. You may also cease being in the research at any time without any consequences.

Discomfort and risks

Some of the queries will be on intimate subjects and may be embarrassing or may cause you some discomfort. If this happens, you may refrain from answering these questions if you so choose. You may also halt the interview at any time.

Benefits

Your participation in this project will allow us to comprehend and capture challenges experienced in using Information Security Metrics to improve patient safety. The information you provide will enable the researcher to make suggest possible modifications needed to healthcare providers.

Reward

There will be no financial benefits for engaging in this project.

Confidentiality

Your name shall not be written on the questionnaire. The questionnaires will be safeguarded by the researcher and confidentiality shall be maintained.

Contact information

For any queries you have, contact Dr. Bernard Muiya on 0722980511 or the Kenyatta University Ethical Review Committee secretariat on chairman.kuerc@ku.ac.ke, secretary.kuerc@ku.ac.ke, ercku2008@gmail.com.

Participant's statement

The details above regarding my involvement in the study are clear to me. I have been granted an opportunity to ask questions and my queries have been addressed satisfactorily. My engagement in this project is voluntary. I understand that my records will remain private and that I can terminate the study at any time.

Name of participant _____

Signature _____

Date _____

Investigator's statement

I, the undersigned, have described to the volunteer in a language s/he understands the process to be followed in the study and the perils and rewards involved.

Name of interviewer _____

Interviewer's signature _____

Date _____

Appendix II: Research Questionnaire

INTRODUCTION

My name is **Maryanne Waithera Mwaura**, a post graduate student at Kenyatta University pursuing Masters of Security Management and Police Studies. To fulfil the program requirements, I am conducting a research project on: The challenges in using Information Security Metrics to improve patient safety in public medical institutions, in Nairobi Metropolitan, Kenya. The information you offer will be used solely for academic intents and shall be treated with utmost confidentiality.

SECTION A: BACKGROUND INFORMATION

Please put a mark (x) in the box next to the right response and where applicable write brief responses in the spaces provided.

1. Sex:
   A) Male ☐
   B) Female ☐
2. Please give your age in the box below:

   ☐
3. What is your professional body? Tick one

No	PROFESSIONAL BODY	RESPONSE
1.	Nursing Officer	
2.	Clinical Officer	

3.	Community Oral Health Officer	
4.	Dentist	
5.	Medical Doctor	
6.	Medical consultant specialist	
7.	Laboratory Officer	
8.	Physiotherapist/Occupational health	
9.	Radiologist/Radiographer	
10.	Pharmacist/Pharm Technologist	
11.	Mental Health Officer	

4. What is your highest level of education (tick where appropriate)

Education Level	
Certificate level	
Diploma	
Higher diploma	
Undergraduate	
Masters	
Doctorate	

5. Please indicate the hospital where you are currently working

a. Public Hospital:

Kenyatta National Hospital	
Spinal Injury referral Hospital	
Mathari National teaching and referral Hospital	
Kenyatta University teaching and referral hospital	

6. How long have you worked in this hospital?

7. Which hospital department do you work in?

Department	
a. Dental services	
b. Eye unit	
c. Medical records	
d. Pharmacy services	
e. Laboratory and diagnostics	
f. Casualty and emergency services	
g. Medical imaging and diagnostics	
h. Maternity services	

i. Child health services	
j. Intesive care and theatre services	
k. Medical ward	
l. Surgical ward	

8. Do you have an education background in computer applications?
    a. Yes ☐
    b. No ☐
9. If No to question 8 above, does it affect how you interact with ISM?
    a. Yes ☐
    b. No ☐
10. Concerning your healthcare facility, do you hold any administrative position?
    a. Yes ☐
    b. No ☐
11. If Yes to question 10 above, does the position allow you to make vital ISM decisions that help improve patient safety?
    a. Yes ☐
    b. No ☐
12. How many computers are available in your department for patient data collection purposes?**(to be answered by those in administrative positions only)**

    ☐

13. How would you rate the overall use of ISM in this hospital?
    a. Poor ☐
    b. Fair ☐
    c. Good ☐
    d. Excellent ☐

14. In the past 12 months, what type of ISM issues have you encountered in your clinical practice in this hospital, kindly tick the appropriate response below:

No.	Statement	Yes	No
a.	Technical glitch in data collection software		
b.	Missing patient information in data collection software		
c.	Incorrect patient information in data collection software		
d.	Ads and unnecessary information while using data collection software		
e.	Inability to access patient information despite having clearance		

15. If yes to question 11 above, how did you handle the ISM issue?
    a. Alerted a supervisor ☐
    b. Alerted a colleague ☐
    c. Alerted the hospital management ☐
    d. Left the matter to settle on its own ☐
    e. Was not sure what to do ☐

16. Concerning ISM in this healthcare facility, what would you attribute as the most common cause of medical errors in this healthcare facility? (**choose the most likely**)

    a. Patient information not available at the right time ☐

b. Lack of managerial support in using ISM

c. Inadequate ISM skills among healthcare workers ☐

d. Inadequate ISM reporting systems that deal with patient safety ☐

e. Lack of ISM culture in the organization ☐

17. **SECTION B: TECHNICAL COMPONENTS**

Concerning technical components, please indicate your agreement or disagreement with the following statements about your hospital (where 1-strongly disagree, 2-disagree, 3-neutral, 4-agree, 5-strongly agree)

Statements on technical components	**LEVEL OF AGREEMENT**				
	1 Strongly disagree	**2 Disagree**	**3 Neutral**	**4 Agree**	**5 Strongly agree**
This healthcare facility has a data collection software where patient data is collected and stored					
The healthcare staff in this hospital are adequately trained in use of ISM					
The hospital management prioritizes use of ISM in promoting patient safety					
For this health care facility, computers, laptops, Ipads are					

adequately available for the access and storage of patient information					
For this health care facility, a back up generator is available to power up computers that are used in storage of patient information					
This healthcare facility has stand by technicians that handle any technical issues arising in the use of ISM					
This healthcare facility addresses technical issues regarding ISM promptly and swiftly					
There is a culture of organizational learning and evidence based decision making from patient data collected in this hospital					
In this healthcare facility culture of using ISM is practiced					

18. Do you have any other issues that affect ISM technical components in your hospital……

……
……
……

19. SECTION C: SECURITY CONTROLS

Concerning ISM security controls, please indicate your agreement or disagreement with the following statements about your hospital (where 1-strongly disagree, 2-disagree, 3-neutral, 4-agree, 5-strongly agree)

Statements on security controls	**LEVEL OF AGREEMENT**				
	1 Strongly disagree	**2 Disagree**	**3 Neutral**	**4 Agree**	**5 Strongly agree**
In this healthcare facility, it is okay to share computer passwords with others					
In this healthcare facility the computers are firewall enabled					
In this healthcare facility the computers have an up to date anti-virus					
This healthcare facility has proper system access control					

mechanisms like user accounts					
In this facility patient data is adequately protected from illegal access and accidental loss					
There are security controls present that protect data storage assets from theft and hacking					

20. Do you have any other ISM security controls issues that affect patient safety……
……
……
……

21. SECTION D: REPORTING SYSTEMS

Concerning ISM reporting systems, please indicate your agreement or disagreement with the following statements about your hospital (where 1-strongly disagree, 2-disagree, 3-neutral, 4-agree, 5-strongly agree)

Statements on ISM reporting systems	**LEVEL OF AGREEMENT**				
	1 Strongly disagree	**2 Disagree**	**3 Neutral**	**4 Agree**	**5 Strongly agree**

In this hospital, healthcare workers are provided with conducive environment for reporting ISM incidences that affect patient safety					
The hospital management has invested in reporting systems that capture ISM related issues					
In this healthcare facility reporting of ISM related issues is mandatory					
Hospital staff are alerted promptly when data softwares are undergoing upgrades in their department					
The hospital management encourages reporting of ISM related issues					
In this healthcare facility there is a targeted patient safety incident report procedure for ISM related issues					
In this healthcare facility hospital management uses the reported cases to make evidence based decisions					

22. Do you have any other ISM reporting systems issues that affect patient safety……
……

……

……

23. SECTION E: LEGAL ASPECTS

Concerning ISM legal aspects, please indicate your agreement or disagreement with the following statements about your hospital (where 1-strongly disagree, 2-disagree, 3-neutral, 4-agree, 5-strongly agree)

Statements on ISM legal aspects	**LEVEL OF AGREEMENT**				
	1 Strongly disagree	**2 Disagree**	**3 Neutral**	**4 Agree**	**5 Strongly agree**
In this hospital, patient engagement and approval in data collection is granted beforehand.					
In this healthcare facility patients are actively engaged in the data collection process					
In this hospital patient data privacy and confidentiality is prioritized					
In this hospital there are data policies that protect the confidentiality, availability and integrity of patient data					

In this hospital there are legal implications for sharing/altering of patient information without consent					

24. How would you rate the overall patient safety in this hospital?
    a. Poor ☐
    b. Fair ☐
    c. Good ☐
    d. Excellent ☐

THANK YOU!

Appendix III: Interview guide

Introduction

My name is **Maryanne Waithera Mwaura**, a post graduate student at Kenyatta University pursuing Masters of Security Management and Police Studies. To achieve the program requirement, I am conducting a research project on: The challenges in using Information Security Metrics to improve patient safety in public medical centers, in Nairobi Metropolitan, Kenya. The information you offer will be used solely for academic intents and will be treated with utmost confidentiality.

Public Hospital:

☐ Kenyatta National Hospital

☐ Spinal Injury refferal Hospital

☐ Mathari National teaching and referral Hospital

☐ Kenyatta University teaching and referral hospital

Department:

☐ ICT

☐ Health records

Interview guide:

1. Which data collection methods are used in the hospital?

2. What data collection software is used to collect, analyse and store patient data in the hospital?

3. What are the security procedures put in place to protect patient data in the hospital?

4. Is there health care staff training in using ISM to promote patient safety in the hospital?

5. Are there updated and on site refresher courses administered on healthcare staff to keep in pace with the ever changing technology?

6. Giving your own opinion does health care staff training on ISM, hospital security culture on data collection, reporting procedures and managerial influence on use of ISM affect patient safety?

7. What challenges does the hospital encounter in the use of ISM to improve patient safety in the hospital?

Appendix III: Introductory letter

TITLE: CHALLENGES IN USING INFORMATION SECURITY METRICS TO IMPROVE PATIENT SAFETY IN PUBLIC HOSPITALS, NAIROBI METROPOLITAN, KENYA

Serial number: _____

Start time: _____ End time: _____

My name is Maryanne Waithera Mwaura, a post graduate student in the Security and Correctional Science Department, Kenyatta University pursuing Masters of Security Management and Police Studies. I shall be conducting a study on: The challenges of using Information Security Metrics to improve patient safety in public hospitals, in Nairobi Metropolitan, kenya. This is a significant study targeting the healthcare sector.

The exercise shall be conducted in Nairobi Metropolitan. The discussion is estimated to take 10 minutes. The information you offer will enable us to comprehend the challenges of using Information Security Metrics to improve patient safety.

The information you offer is private and will not be share with anyone. It will only be employed for research purposes. Your involvement is voluntary and you are free to decline answering any questions in the questionnaire. In case you have any queries about the study, you may ask me (0796618367) or contact the Chairman, Security and Correctional Sciences at chairperson-scs@ku.ac.ke. There are no financial benefits for participating in the activity but you may benefit since the project will help in identifying the challenges faced in using ISM to enhance patient safety. You are free at any time to stop participating in the exercise.

Appendix IV: NACOSTI License

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **983643**

Date of Issue: **12/May/2022**

RESEARCH LICENSE

This is to Certify that Miss.. Maryanne Waithera Mwaura of Kenyatta University, has been licensed to conduct research in Nairobi on the topic: Challenges in Using Information Security Metrics to Improve Patient Safety in Public Hospitals, Nairobi County, Kenya. for the period ending : 12/May/2023.

License No: **NACOSTI/P/22/17412**

983643

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.

Appendix V: KUERC Aprroval Letter

KENYATTA UNIVERSITY
CENTRE FOR RESEARCH ETHICS AND SAFETY

Fax: 8711242/8711575 **P. O. Box 43844,**
Email: chairman.kuerc@ku.ac.ke
Nairobi, 00100

Tel: 8710901/12

Website: www.ku.ac.ke
Our Ref: **KU/ERC/APPROVAL/VOL.1** Date: 5th /07/2022

Maryanne Mwaura
P.O Box 43844, 00100
Nairobi.

Dear Ms.Mwaura,

APPLICATION NUMBER: PKU/2527/I1654- CHALLENGES IN USING INFORMATION SECURITY METRICS TO IMPROVE PATIENT SAFETY IN PUBLIC HOSPITALS IN NAIROBI CITY COUNTY, KENYA

This is to inform you that ***KENYATTA UNIVERSITY ETHICS REVIEW COMMITTEE*** has reviewed and approved your above research proposal. Your application approval number is **PKU/2527/I1654.** The approval period is **5th /07/2022 *to* 5th /07/2023**

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 ***KENYATTA UNIVERSITY ETHICS REVIEW COMMITTEE***
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 ***KENYATTA UNIVERSITY ETHICS REVIEW COMMITTEE*** within 72 hours of notification
iv. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to ***KENYATTA UNIVERSITY ETHICS REVIEW COMMITTEE*** within 72 hours
v. Clearance for export of biological specimens must be obtained from relevant institutions.

Appendix VI: Declining Email From KUTRRH

Deputy Director... 8/16/2022
to me, Marion, Wangari

Dear Maryanne,

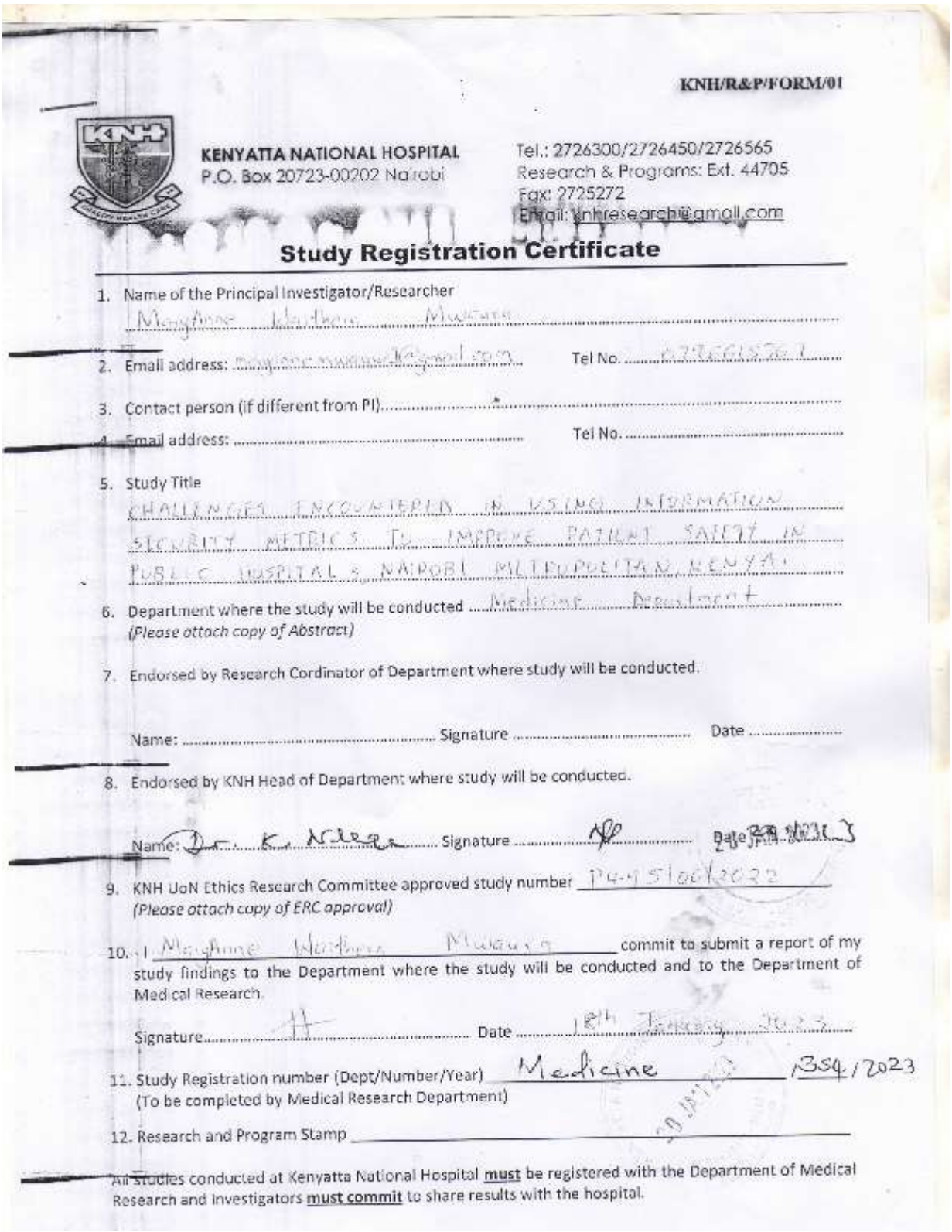
I trust that this finds you well.
Regarding your request to carry out research within KUTRRH, we regret to inform you that due to some unavoidable circumstances, data collection in the hospital has been halted until further notice. We sincerely apologize for any inconveniences this may cause.

Regards,

Dr. Marion Wangui Kigutya.
Deputy Director Research and Clinical Trials.
Kenyatta University Teaching, Referral & Research Hospital

Located at: Northern Bypass Rd., Kahawa West, Nairobi
Website: www.kutrrh.go.ke
Email: info@kutrrh.go.ke
Twitter: @kutrrh | Facebook: @kureferral | Instagram: @kureferral
LinkedIn: KUTRRH

Appendix VII: KNH Registration Certificate



KNH/R&P/FORM/01

KENYATTA NATIONAL HOSPITAL
P.O. Box 20723-00202 Nairobi

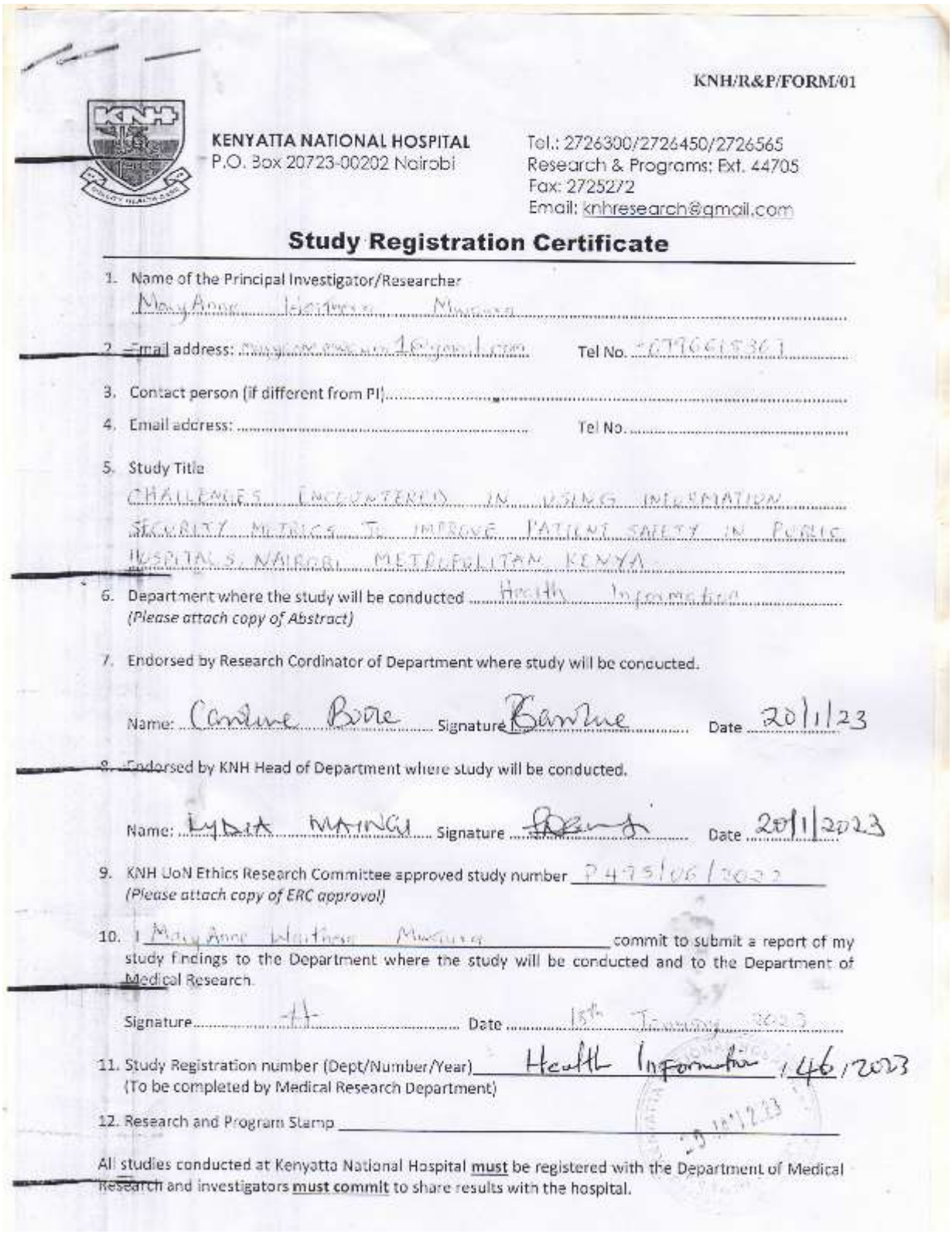
Tel.: 2726300/2726450/2726565
Research & Programs: Ext. 44705
Fax: 2725272
Email: knhresearch@gmail.com

Study Registration Certificate

1. Name of the Principal Investigator/Researcher
   Maryanne Wambua Mwaura
2. Email address: maryanne.mwaura@gmail.com Tel No. 0726613261
3. Contact person (if different from PI).....
4. Email address: ..... Tel No. .....
5. Study Title
   CHALLENGES ENCOUNTERED IN USING INFORMATION SECURITY METRICS TO IMPROVE PATIENT SAFETY IN PUBLIC HOSPITALS NAIROBI METROPOLITAN KENYA.
6. Department where the study will be conducted Medicine Department
   (Please attach copy of Abstract)
7. Endorsed by Research Cordinator of Department where study will be conducted.
   Name: ..... Signature ..... Date .....
8. Endorsed by KNH Head of Department where study will be conducted.
   Name: Dr. K. Nderu Signature ..... Date 23/1/2023
9. KNH UoN Ethics Research Committee approved study number P4-5/oct/2022
   (Please attach copy of ERC approval)
10. I Maryanne Wambua Mwaura commit to submit a report of my study findings to the Department where the study will be conducted and to the Department of Medical Research.
    Signature ..... Date 18th January 2023
11. Study Registration number (Dept/Number/Year) Medicine /354/2023
    (To be completed by Medical Research Department)
12. Research and Program Stamp

All studies conducted at Kenyatta National Hospital **must** be registered with the Department of Medical Research and investigators **must commit** to share results with the hospital.

Appendix VIII: KNH Registration Certificate



KNH/R&P/FORM/01

KENYATTA NATIONAL HOSPITAL
P.O. Box 20723-00202 Nairobi

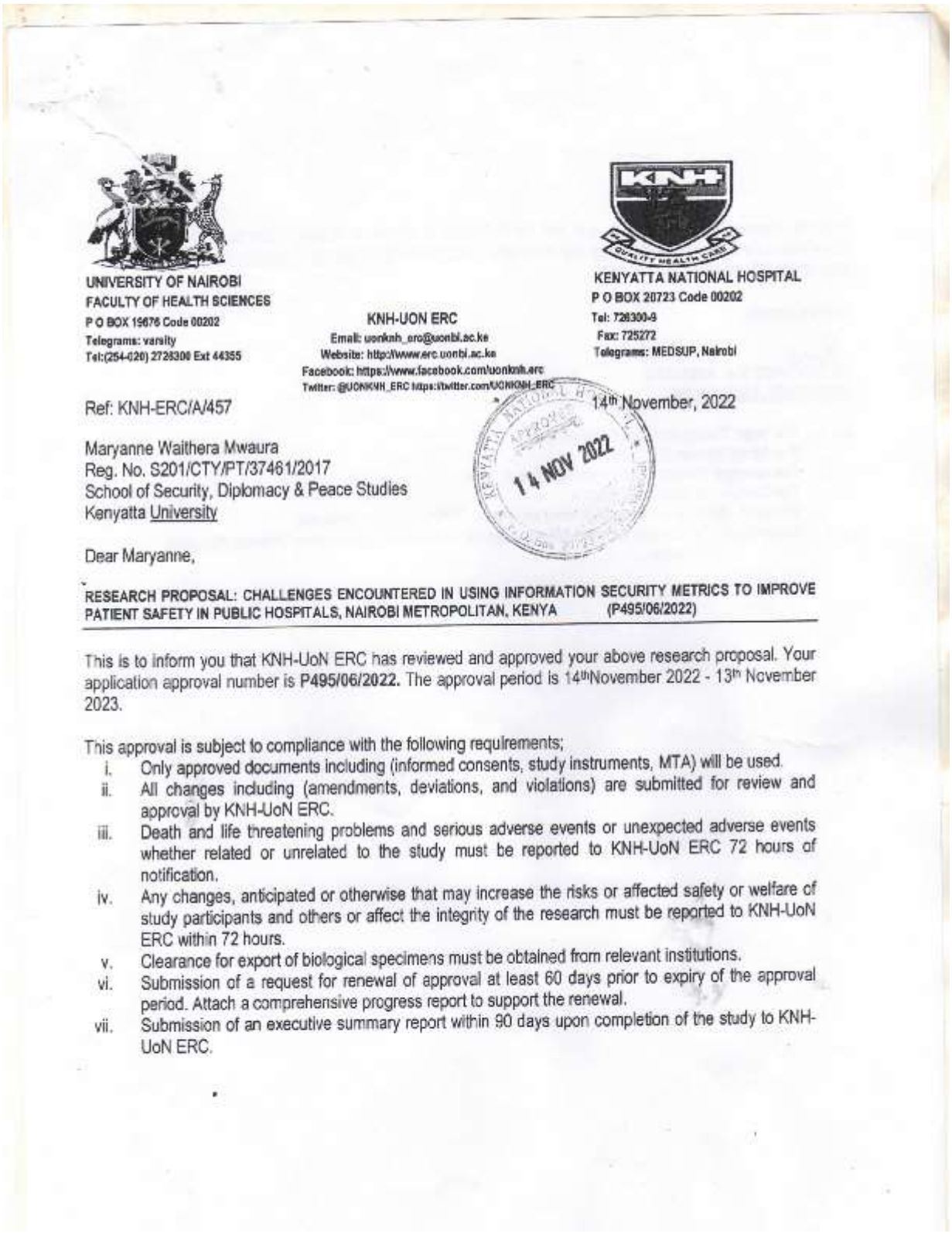
Tel.: 2726300/2726450/2726565
Research & Programs: Ext. 44705
Fax: 2725272
Email: knhresearch@gmail.com

Study Registration Certificate

1. Name of the Principal Investigator/Researcher
   Mary Anne Wairimu Mwaura
2. Email address: [illegible] Tel No. [illegible]
3. Contact person (if different from PI) .....
4. Email address: ..... Tel No. .....
5. Study Title
   CHALLENGES ENCOUNTERED IN USING INFORMATION SECURITY METRICS TO IMPROVE PATIENT SAFETY IN PUBLIC HOSPITALS, NAIROBI METROPOLITAN KENYA
6. Department where the study will be conducted Health Information
   (Please attach copy of Abstract)
7. Endorsed by Research Cordinator of Department where study will be conducted.
   Name: Caroline Bore Signature Caroline Date 20/1/23
8. Endorsed by KNH Head of Department where study will be conducted.
   Name: LYDIA MAINGI Signature [signature] Date 20/1/2023
9. KNH UoN Ethics Research Committee approved study number P475/06/2022
   (Please attach copy of ERC approval)
10. I Mary Anne Wairimu Mwaura commit to submit a report of my study findings to the Department where the study will be conducted and to the Department of Medical Research.
    Signature [signature] Date 18th January 2023
11. Study Registration number (Dept/Number/Year) Health Information/46/2023
    (To be completed by Medical Research Department)
12. Research and Program Stamp [illegible]

All studies conducted at Kenyatta National Hospital must be registered with the Department of Medical Research and investigators must commit to share results with the hospital.

Appendix IX: KNH-UON ERC Aprroval Letter



UNIVERSITY OF NAIROBI
FACULTY OF HEALTH SCIENCES
P O BOX 19676 Code 00202
Telegrams: varsity
Tel:(254-020) 2726300 Ext 44355

KNH-UON ERC
Email: uonknh_erc@uonbi.ac.ke
Website: http://www.erc.uonbi.ac.ke
Facebook: https://www.facebook.com/uonknh.erc
Twitter: @UONKNH_ERC https://twitter.com/UONKNH_ERC

KENYATTA NATIONAL HOSPITAL
P O BOX 20723 Code 00202
Tel: 726300-9
Fax: 725272
Telegrams: MEDSUP, Nairobi

Ref: KNH-ERC/A/457

14th November, 2022

APPROVED
14 NOV 2022

Maryanne Waithera Mwaura
Reg. No. S201/CTY/PT/37461/2017
School of Security, Diplomacy & Peace Studies
Kenyatta University

Dear Maryanne,

RESEARCH PROPOSAL: CHALLENGES ENCOUNTERED IN USING INFORMATION SECURITY METRICS TO IMPROVE PATIENT SAFETY IN PUBLIC HOSPITALS, NAIROBI METROPOLITAN, KENYA (P495/06/2022)

This is to inform you that KNH-UoN ERC has reviewed and approved your above research proposal. Your application approval number is **P495/06/2022.** The approval period is 14th November 2022 - 13th November 2023.

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 KNH-UoN ERC.
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 KNH-UoN ERC 72 hours of notification.
iv. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to KNH-UoN ERC 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 KNH-UoN ERC.

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

Yours sincerely,

DR. BEATRICE K.M. AMUGUNE
SECRETARY, KNH-UoN ERC

c.c. The Dean, Faculty of Health Sciences, UoN
The Senior Director, CS, KNH
The Assistant Director, Health Information Dept., KNH
The Chairperson, KNH- UoN ERC
The Dean, School of Security, Diplomacy and Peace Studies, Kenyatta University
Supervisors: Dr. Bernard Munayo Mulya, Dept .of Security and Corrections Science, Kenyatta University

Appendix X: Mathari Referral Research Invoice

MATHARI NATIONAL TEACHING AND REFERRAL HOSPITAL

P.O BOX 4[illegible]-00100 ,

07722094[illegible]

Debtor Invoice #DI184 -Training

Print Date: 22/03/2022 10:[illegible] AM

Debtor Invoice

InvNo : **#DI184**

Training

Name of Payer: MARYANN WAITHERA — Scheme: Aga Khan University

ID.	Department	Service	Qty	Unit Item Amount	S.Amount
2.4	ADMINISTRATION	AI SEARCH FOR MASTERS AND ABOVE		2,000.00	2,000.00

Total Amnt: 2,000.00

MATHARI NATIONAL TEACHING & REFERRAL HOSPITAL — 23 JUN 2022 — INVOICED

Sign: [signature]

Sign By:

Date: 23/6/22

Appendix XI: Mathari Clearance Form

MATHARI HOSPITAL

CLEARANCE TO UNDERTAKE RESEARCH IN MATHARI HOSPITAL

TO: ALL THE DEPARTMENTAL HEADS Dates 23/6/2022

This is to inform you that (name/no. of students)

MARYANN WAITHERA MWAURA

From (Name of training institution)

K.U

Has/have been cleared by the office of the Medical Superintendent to undertake research at Mathari hospital
from 23/6/2022 to 23/7/2022

Please accord them/him/her ✓ the necessary support.

DECLARATION

I Maryanne Waithera Mwaura commit myself to bring back a final copy of the research to Mathari National Teaching and Referral Hospital.

Name: GRACE KINENA

In-Charge C.M.E.D

Appendix XII: KNH Medicine Depatment Approval Letter

KENYATTA NATIONAL HOSPITAL
P.O. BOX 20723, 00202 Nairobi

Tel.: 2726300/2726450/2726550
Fax: 2725272
Email: knhadmin@knh.or.ke

Ref: KNH/HOD-MED/37/VOL.II

Date: 19th January 2023

Maryanne Waithera Mwaura
Reg. No. S201/CTY/PT/37461/2017
School of Security, Diplomacy & Peace Studies
Kenyatta University

Dear Maryanne,

RE: APPROVAL TO CONDUCT A STUDY AT THE KNH MEDICINE DEPARTMENT

Following approval by the KNH/UON-Ethics & Research Committee for your research proposal and subsequent filing of the study registration certificate, this is to inform you that authority has been granted to collect data in Medicine Department, on your study titled ***"Challenges encountered in using information security metrics to improve patient safety in public hospitals, at Kenyatta National Hospital, Nairobi County "***

By a copy of this letter, **DCN - Medical Services** is informed and requested to facilitate.

You will also be required to submit a report of your study findings to the office of the undersigned after completion of your study.

Dr. Kinoti Ndege
HOD, MEDICINE

DCN - Medical Services

Appendix XIII: Confirmation of Studentship

KENYATTA UNIVERSITY

OFFICE OF THE REGISTRAR (ACADEMIC)

FAX: 811242/811575
Email: admissions-pg@ku.ac.ke
Website: www.ku.ac.ke

P.O Box 4384400100
NAIROBI, KENYA
Tel: 020-870 3223/0780830830

OUR REF: S201/CTY/PT/37461/2017 DATE: 19th May, 2022

TO WHOM IT MAY CONCERN

RE: CONFIRMATION OF STUDENTSHIP , MWAURA MARYANNE WAITHERA
REG. NO S201/CTY/PT/37461/2017

This is to confirm that the above named is a bonafide student of Kenyatta University admitted in January, 2017 to pursue a Master of Arts in Security Management and Police Studies on Part Time mode of Study.

Ms. Mwaura has completed her coursework and needs to embark on her Research Project that entails data collection and project writing.

Kindly accord her the necessary support she may require to complete her course.

Sincerely,

MR. R. A. CHWEYA
FOR REGISTRAR (ACADEMIC)

RC/jw

Appendix XIV: Graduate School Letters

KENYATTA UNIVERSITY
GRADUATE SCHOOL

E-mail: dean-graduate@ku.ac.ke
Website: www.ku.ac.ke

P.O. Box 43844, 00100
NAIROBI, KENYA
Tel. 8710901 Ext. 57530

Our Ref: S201/CTY/PT/37461/2017

DATE: 8th April, 2022

Director General,
National Commission for Science, Technology
and Innovation
P.O. Box 30623-00100
NAIROBI

Dear Sir/Madam,

RE: RESEARCH AUTHORIZATION FOR MARYANNE WAITHERA MWAURA – REG. S201/CTY/PT/37461/2017

I write to introduce **Maryanne Waithera Mwaura** who is a Postgraduate Student of this University. The student is registered for M.A degree programme in the **Department of Security and Correction Science.**

Maryanne intends to conduct research for a M.A Project Proposal entitled, **"Challenges in Using Information Security Metrics to Improve Patient Safety in Public Hospitals, Nairobi County, Kenya."**

Any assistance given will be highly appreciated.

Yours faithfully,

KENYATTA UNIVERSITY OFFICE OF DEAN 19 MAY 2022 GRADUATE SCHOOL P.O. BOX 43844 - 00100 NAIROBI

PROF. ELISHIBA KIMANI
DEAN, GRADUATE SCHOOL

Jl/mg

KENYATTA UNIVERSITY
GRADUATE SCHOOL

E-mail: dean-graduate@ku.ac.ke
Website: www.ku.ac.ke

P.O. Box 43844, 00100
NAIROBI, KENYA
Tel. 810901 Ext. 4150

Internal Memo

FROM: Dean, Graduate School

DATE: 8th April, 2022

TO: **Maryanne Waithera Mwaura**
C/o Security & Correction Science Dept.

REF: S201/CTY/PT/37461/2017

SUBJECT: APPROVAL OF RESEARCH PROPOSAL

We acknowledge receipt of your revised Research Proposal as per our recommendations raised by the Graduate School Board of 2nd March, 2022 entitled **"Challenges in Using Information Security Metrics to Improve Patient Safety in Public Hospitals, Nairobi County, Kenya."**

You may now proceed with your Data Collection, Subject to Clearance with Director General, National Commission for Science, Technology and Innovation.

As you embark on your data collection, please note that you will be required to submit to Graduate School completed Supervision Tracking and progress report forms per semester. The forms are available at the University's Website under Graduate School webpage downloads.

Thank you.

KENYATTA UNIVERSITY OFFICE OF DEAN 19 MAY 2022 GRADUATE SCHOOL P.O. BOX 43844-00100 NAIROBI

JACKSON LUVUSI
FOR: DEAN, GRADUATE SCHOOL

C.c. Chairman, Department of Security and Correction Science

Supervisors:

1. Dr. Bernard Munyao Muiya
   C/o Department of Security and Correction Science
   Kenyatta University

JL/mo