ELECTRONIC HEALTH SYSTEM INTEGRATION FRAMEWORK FOR SECURE M-HEALTH SERVICES: A CASE STUDY OF UNIVERSITY OF NAIROBI HOSPITAL

NANDASABA SAMUEL

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR AWARD OF THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY OF

MOUNT KENYA UNIVERSITY

NOVEMBER 2024

DECLARATION AND APPROVAL

DECLARATION:

This research proposal is my own original work and to the best of my knowledge, it has not been submitted for a degree in any other University.

Signed:  **Date: 09/09/2024**

SAMUEL NANDASABA

Reg No: MIT/2013/50898

APPROVAL:

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

Signed:  **Date: 03/10/2024**

Prof. Gregory Wanyembi **(**Mount Kenya University)

Signed:  **Date: 11/10/2024**

Dr. Geoffrey Mariga **(**Murang'a University of Technology)

DEDICATION

I dedicate this work to my lovely wife Lucy Namaswa and colleagues for their unwavering support and encouragement.

ACKNOWLEDGEMENT

Thanks to the Almighty God, for granting me strength and good health to complete this thesis.

I would also like to thank the Mount Kenya University fraternity for offering me a conducive environment to do my postgraduate studies.

I'm most grateful to my supervisors Prof. Wanyembi and Dr Geoffrey Mariga for guiding me throughout the study and for their patience and dedication for the entire process. Their immense skills and knowledge of the subject matter enabled me to shape this project properly to completion.

ABSTRACT

The purpose of this research sought to design a secure framework that can be used in M-Health systems development. The researcher used the integrated information theory as a framework for enforcing system security as a holistic approach. To actualize this study, objectives that were meant to guide in carrying out the research were: To evaluate the significance of Confidentiality, Integrity and availability on the security of M-health systems, develop a framework for secure integration of M-Health systems and validate the proposed framework**.** The researcher used University of Nairobi Hospital because it had Implemented E health system for more than ten years and therefore more data was available for collection and analysis to conduct the research. The study adopted a case study design methodology that included a sample size of forty-four (44) ICT personnel and users of University Health System at the University of Nairobi Hospital. The methodology employed in this research was case study design. A systematic random sampling technique was applied in this study. Data collection methods were observation, conducting interviews and filling questionnaires that were administered to the target population in the University of Nairobi Hospital. It was established that there was significant comprehensive security in the University of Nairobi Health system. In addition, introduction of Pseudonymization to EMRs enhanced patient data security. A secure integration framework was also designed in the study. Recommendations were made to the university of Nairobi Hospital to address the gap of Pseudonymization of patients records in the University Health system. A model was developed and tested using a prototype that was developed using C#, ASP.NET framework, IDE Visual Studio and SQL Server.

TABLE OF CONTENTS

DECLARATION AND APPROVAL ii

DEDICATION iii

ACKNOWLEDGEMENT iv

ABSTRACT v

TABLE OF CONTENTS vi

LIST OF FIGURES xiv

LIST OF TABLES xvii

LIST OF ABBREVIATIONS AND ACRONYMS xix

CHAPTER ONE 1

1. INTRODUCTION 1

1.1 Background of the study 1

1.1.1 E- Health 4

1.2 Problem Statement 5

1.3 Research Objectives 7

1.3.1 Main Objective 7

1.3.2 Specific Objectives 7

1.3.3 Research Questions 7

1.4 Justification of the study 8

1.5 Significance of the study 9

1.6 Scope of the study. 9

1.7 Study limitations. 10

1.8 Structure of the thesis 11

CHAPTER TWO 12

2. LITERATURE REVIEW 12

2.1 Introduction 12

2.2 Theoretical Framework 12

2.2.1 CIA Triad in Electronic Medical Record Systems 13

2.2.2 The integrated systems theory 15

2.3 ICT and Healthcare systems 21

2.4 Existing frameworks for M-Health Systems..... 22

2.4.1 A framework for assessing M-Health challenges in South Africa. 22

2.4.2 M-Health decision making framework for community-based services 25

2.4.3 Mobile Application Security System Framework..... 28

2.4.4 A framework to improve mobile banking security. 31

2.4.5 An Enhanced Mobile Health Applications Cloud Computing Framework 33

2.4.6 Secure mobile data collection system framework. 35

2.4.7 SecourHealth Framework. 37

2.5 Conceptual framework..... 38

2.5.1 Confidentiality 40

2.5.2 Integrity 44

2.5.3 Availability 49

2.5.4 Pseudonymization. 54

2.5.5 Standards and Regulations 60

2.5.6 Common Data Security Architecture 63

2.5.7 Summary of literature review 69

CHAPTER THREE 74

3. RESEARCH METHODOLOGY 74

3.1 Introduction 74

3.2 Study Design 75

3.3 Study Population and sample size determination. 75

3.4 Pre-test 79

3.5 Testing for validity and reliability 79

3.6 Data Collection 79

3.7 Data Management 80

3.8 Data Analysis and Presentation 80

3.8.1 Correlation analysis technique: 80

3.8.2 Regression Analysis technique: 81

3.8.3 Ethical Considerations 82

CHAPTER FOUR 83

4. RESEARCH FINDINGS AND DISCUSSIONS 83

4.1 Results 84

4.2 Relationship between independent variables on Security of M-Health Systems 100

4.2.1 Correlation Analysis 100

4.2.2 Regression Analysis 101

4.3 Discussion of Findings 105

4.4 Framework Design. 106

4.4.1 Requirement Analysis 106

4.4.1.1 Security Requirements 106

4.4.1.2 Interoperability Requirements 107

4.4.2 Framework Architecture 108

4.4.2.1 Modular Design 108

4.4.2.2 Secure APIs 109

4.4.2.3 Encryption Methods 110

4.4.2.4 Data Integrity Mechanisms 110

4.4.3 Security Features 111

4.4.3.1 Multi-Factor Authentication (MFA) 111

4.4.3.2 Secure Communication Protocols 111

4.4.3.3 Access Control and Authorization 112

4.4.4 Interoperability Considerations 112

4.4.4.1 Adoption of HL7 and FHIR Standards 112

4.4.4.2 Data Mapping and Transformation 113

4.4.4.3 Scalability and Extensibility 113

4.5 Basic Pseudonymization Technique 116

4.6 Validation of the proposed framework 119

CHAPTER FIVE 120

5. SUMMARY ,CONCLUSIONS AND RECOMMENDATIONS 120

5.1. Introduction 120

5.2. Summary of findings 120

5.3. Conclusion 121

5.4. Future research recommendations 122

REFERENCES 123

APPENDICES 130

i. Ethics review committee Certificate. 131

ii. Introduction Letter from postgraduate 132

iii. Approved certificate from NACOSTI. 133

iv. Informed Consent form 134

v. Interview Schedule 136

vi. Questionnaire 137

vii. Turnitin Report 140

viii. Pseudonymization code 133

ix. Publication 163

x. Pseudonym Flow Chart 164

LIST OF FIGURES

Figure 1: M-Health Architecture (Bourouis et al., 2012) 3

Figure 2: Integrated system Theory (Adapted from Hong et al. 2003) 16

Figure 3:A framework for assessing M-Health challenges in South Africa (Leon et al, 2012) 24

Figure 4: Data transfer using encryption and digital signatures. (Maranda,2016) 26

Figure 5: Components of the iSec framework. (Maranda, 2016). 28

Figure 6: Analyzed hashes obtained for the conflicting parties. (Floyd, 2006)) 30

Figure 7: Corrupt application identified by consensus vote (Floyd, 2006) 30

Figure 8: Termination of corrupt application from the network. (Floyd, 2006)..... 31

Figure 9: Secure M-banking model ((Source, Elkhodr (2012))..... 32

Figure 10: Secure mobile banking approach framework activity diagram. (Elkhodr, 2012) 33

Figure 11: A framework of IP multimedia subsystem standard –based mobile health monitoring with cloud support. (Nkosi& Mekuria, 2010)..... 35

Figure 12:showing the modules and the explanation (Gejibo,2015) 37

Figure 13: Conceptual framework, Researcher 2024. 39

Figure 14: Period for which respondents have worked in the hospital. 86

Figure 15: Academic qualification for the respondents 87

Figure 16:Timely updating of records 88

Figure 17:Accuracy of medical records through protection against data loss 89

Figure 18: Security of medical records while in transmission. 90

Figure 19:Basic IT Skills or knowledge 92

Figure 20:Password protection of computers. 93

Figure 21:Protection of data through roles and rights of access to patients data. 94

Figure 22: System availability. 95

Figure 23:Traceability flow of information. 96

Figure 24:Offsite backup. 97

Figure 25: Accessibility of patient data by medical professionals 98

Figure 26:Computer Antivirus protection. 99

Figure 27:Pseudonymized records. 100

Figure 28:Proposed E-Health Security Framework (PEHSF) 115

LIST OF TABLES

Table 1: Sample Population Table for eHealth Framework Study (n=44) 77

Table 2: Academic qualification for the respondents 86

Table 3: Timely addition of medical records in ensuring completeness. 88

Table 4: Response on accuracy of medical records through protection of information against loss. 89

Table 5: Security on medical records while in transmission. 90

Table 6:Responses on whether the Hospital ensured its employees have basic IT knowledge to key in accurate data. 91

Table 7: Protection of data through computer passwords..... 92

Table 8: Protection of data through roles and rights of access to patients' data..... 93

Table 9:Availability of system..... 94

Table 10: Traceability flow of information 95

Table 11: Offsite backup availability..... 96

Table 12:Accessibility of information by medical professionals 97

Table 13: Use of Anti-Virus 98

Table 14:Patient records Pseudonymized. 99

Table 15: Correlation Analysis 101

Table 16:Model Summary 102

Table 17:Anova (Analysis of Variance) 102

Table 18:Coefficient of Determination 103

Table 19:Basic Pseudonymization technique 117

Table 20:Pseudonymized data (Health care ID & Name) 117

Table 21:Health ID, healthcare identifier Pseudonym 118

Table 22:Name and name Pseudonym 118

LIST OF ABBREVIATIONS AND ACRONYMS

DPA- Data protection Act

E-health – Electronic Health

EHIS – Electronic Health management information systems

GOK – Government of Kenya

HIPAA- Health Insurance Portability and Accountability Act

ICT – information communication technology

IT – Information Technology

M-Health – Mobile Health

MOH – Ministry of Heath

TLS- Transport Layer Security

UHS- University Hospital System

CHAPTER ONE

1. INTRODUCTION

The purpose of this chapter is to lay the groundwork for the study by providing essential background information. It includes a clear problem statement, outlines the objectives of the research, and presents the research questions guiding the investigation. Additionally, the chapter addresses the justification for the study and its significance, emphasizing its relevance to the field. It also defines the scope of the research, identifying the boundaries within which the study was conducted, and acknowledging any limitations that may impact the findings. Finally, the chapter details the structure of the thesis, offering a roadmap for the reader to navigate the subsequent sections of the work.

1.1 Background of the study

M-Health refers to the use of mobile wireless telecommunications in public health, as defined by the World Health Organization (WHO) in 2017. For M-Health systems to function effectively, they must meet specific conditions related to the wireless environment, including usability, interoperability, link reliability, privacy, security, and resistance to electromagnetic interference. Additionally, the limited resources of mobile devices, such as reduced processing power and small storage capacity, must also be considered.

Despite these requirements, the fundamental advantage of an M-Health infrastructure is its adaptability, which allows the development of health monitoring services beyond traditional healthcare settings like hospitals, dispensaries, or clinics. With M-Health, patients can be monitored

and supported at home, work, or any location with a wireless connection to the communications network.

The concept of M-Health encompasses noninvasive sensors, communication networks, mobile computing, and various healthcare-related technologies, as described by Liu in 2011. One of the primary goals of M-Health is to disseminate health information using widely accessible mobile devices to reach healthcare professionals and organizations, regardless of their distance, as noted by Desai in 2014.

The benefits of remote medicine through M-Health include a reduction in hospitalization costs, the provision of timely and appropriate healthcare, improved patient monitoring processes, structured and centralized patient data, and decreased hospitalization rates in dispensaries, clinics, and hospitals, as highlighted by Berndt in 2011.

M-Health sensors are particularly valuable as they allow for the monitoring of patients' health and physiological data without requiring them to visit a doctor. Furthermore, doctors can access these devices remotely, enabling early detection and effective treatment of chronic diseases, continuous monitoring of patients with existing chronic conditions, and the prevention of such diseases, according to Benharref in 2014.

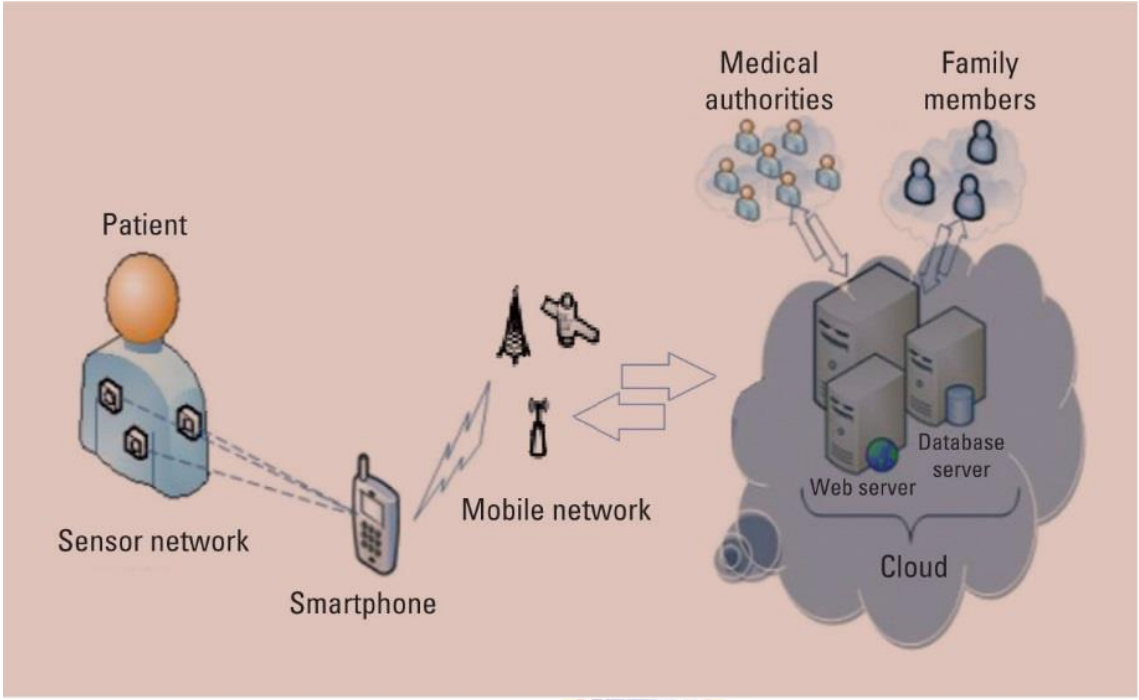


Figure 1: M-Health Architecture (Bourouis et al., 2012)

Communications occur amongst the patient's family, mobile environment, healthcare professionals and the cloud as postulated by Bourouis et al. (2012).

As much as M-Health has come along with many benefits, challenges that never occurred before are now prevalent. Initially systems and their IT components were in controlled environments which were mainly under the administration of specialized teams that might ensure their dependability. The infrastructure dedicated to these systems was common. Since the limits were defined well, the security problems could be easily identified and controlled. When cloud and mobile computing were adopted, the resulting feature was the expansion of these limits and even creation of new challenges that did not occur earlier on.

One of the main concerns for M-Health systems is the assurance of information security that includes confidentiality, availability, authenticity and integrity. This has necessitated the need for development of a secure framework for M-Health systems that the researcher will handle and therefore this framework can be applied by any IT expert in the M-Health systems development.

1.1.1 E- Health

The World Health Organization (WHO) defines E-health as the usage of electronic Information and Communication Technology (ICT) in provision of healthcare services to the patients. For the intent of this project, eHealth is viewed as the use of ICT in all aspects of healthcare, ranging from diagnosis to follow-up. The seventy-first World Health Assembly of WHO (2018) describes E-health as the secure and cost-effective application of ICT to help health and healthcare sector.

According to Blaya et al. (2010) systematic review of eHealth implementations indicates that the best ability for e-health could be in systems that enable prescription ordering and management, promote patient compliance with care regimens, and improve communication between healthcare facilities. The availability and quality of ICT services has increased greatly across Africa. In the late 1990s, mobile network coverage was 16%, it steadily rose to over 90% of the continent's population in 2011. Due to the growth, there has been an increase in investments, a decrease in costs and steady growth in technology-enabled services due to the growth that has been exhibited in this sector. However, the benefits of these improvements in ICT infrastructure haven't been of so much benefit to the health sector in a structured way since most of these projects remain as pilots. Therefore, this study seeks to assess the effect ICT has had on how well healthcare programs have performed in Kenya.

Over the past years ICT has emerged as an essential tool in organizations from a wide range of industries and taking a key role in driving change in both social and economic life (Pernebekova & Ahbergenovich, 2015). Its rapid development has led to the emergence of information society via the utilization of internet and other wireless communications (Wallis, Blessing, Dalwai, & Shin, 2017). The more ICT develops and becomes more available, new opportunities are opened up in the healthcare sector and other industries (Health, 2017). ICT development will inevitably result in the growth of key activities in the healthcare industry since this sector intensively involves information and knowledge. The Kenya health strategic plan for year 2014-2018 aims to ensure quality delivery of health services to all its citizens (Ministry of health, 2016). The plan according to the ministry of health services (MOH) can only succeed with the integration of ICT capabilities to ensuring ease of access as well as ensuring quality of health services by ensuring proper record management as well as accessibility of patient's health information.

1.2 Problem Statement

With the advancement of wireless information technologies and applications, a rapid rise has been recorded in the use of smartphones, tablets, and other electronic gadgets in the health sector. Researchers have developed frameworks such as Maranda (2016), Gejibo (2015), Nkosi (2014)**,** Leon et al. (2012), and Elkhodr (2012). In addressing the M-health information services, these frameworks are faced with security challenges, the major being confidentiality, availability, and integrity, this is negatively affecting the usage of the frameworks in sorting out the security risks. Vimalachandran et al. (2018) noted that because of the effects on encouraging good standards of patient care, maintaining CIA data in EHR systems has grown to be a significant issue. This research therefore aims to offer

an intervention by proposing an integration framework of EHIS into M-health with much focus on the security aspect to enhance M-health applications security. Iwaya et al. (2020) noted that it has become clear that security and privacy are the most difficult parts of healthcare information systems, and it is vital to properly comprehend and handle the security concerns of M-Health.

The Integration of Electronic Medical Records(EMR's) has significantly improved healthcare delivery but has also created a critical challenge in maintaining a delicate balance between ensuring the privacy of patient information and implementing robust security measures .Despite stringent regulations and technological advancements, a substantial gap persists between safeguarding patient data from unauthorized access , breaches or misuse while enabling seamless access for healthcare professionals. This discrepancy poses a threat to patient confidentiality trust in healthcare systems and the integrity of sensitive medical information. Addressing this gap necessitates a comprehensive approach that reconciles stringent security protocols with user friendly access for authorized personnel, ensuring both privacy and security are upheld without compromise. Thus, the research on pseudonymization of the EMR records.

1.3 Research Objectives

The research was guided by the following objectives:

1.3.1 Main Objective

The main objective of this study was to design a framework for electronic health system Integration for secure M-health services at the university of Nairobi hospital.

1.3.2 Specific Objectives

The following three specific objectives served as the study's guide to accomplish the overall goal.

i. To evaluate the significance of a comprehensive information security of M-health systems at the University of Nairobi Hospital.

ii. To design a framework for secure integration of M-Health systems at the University of Nairobi Hospital.

iii. To validate the proposed framework.

1.3.3 Research Questions

i. How can comprehensive information security be realized in an M-health system at the University of Nairobi Hospital?

ii. How can a secure integration framework of M-Health system at the University of Nairobi Hospital be developed?

iii. How do you validate the proposed framework?

1.4 Justification of the study

Cyber security has been a key challenge to computer-based systems in the last few years. It is important to note that systems security should be considered as a part of the system development in any information system and not an implementation requirement. Therefore, the ability to analyze the key security demands of the system and integrate them within the computer-based system as it is being built is critical. Furthermore, for health information systems, preservation of privacy of a patient's health data is one of the key tenets of any health system/facility. Thus, a comprehensive security model must be enforced in any kind of health system for it to be considered effective and beneficial.

The study focused on the influence of electronic health system integration framework for secure m-health services: a case of university of Nairobi hospital. The study adopted a case study design.

Mobile Health applications development plays a crucial role in today's lives with the increasing number of tablets and smartphone users. Mobile technology is growing exponentially and therefore organizations and government are making use of their power to collect, collate, transmit and present data in a timely manner hence overcoming limitations that are in manual systems and the University of Nairobi hospital is not an exception.

Fast growth of mobile technology has made it possible for electronic systems to share data more often, therefore providing decision makers with useful information and improving their capacity to have

very important decisions about health matters. While mobile phone technology has shown tremendous potential to transform health-care distribution, there is little guidance to keep university of Nairobi hospital developers updated about the development of secure frameworks for M-Health systems.

1.5 Significance of the study

This study will enable successful integration of the health information systems with M-health systems in a secure manner. The findings will be used by policymakers as a foundation for the creation of robust information security plans, guidelines, and standards in the creation of hospital systems for improved healthcare delivery. Pseudonymized data can be used for research without compromising patient privacy. Researchers can analyze large datasets to identify trends, develop treatments, and improve healthcare outcomes. It will enable collaboration between institutions and countries by providing a way to share data securely.

The research will be valuable for academicians and scholars since this will contribute to the growing knowledge on information security and will provide reference material to the researchers.

The research will be a basis for further studies around successful E-health integration frameworks for secure M- Health services.

1.6 Scope of the study.

The University of Nairobi is one of the oldest public universities we have in Kenya. It has a student population of more than eighty-four thousand and staff population of more than 7000 both teaching

and non -teaching cadre (University of Nairobi, 2021). It has a level four hospital which serves both students and staff. In this hospital we have a health information system which allows for efficient healthcare service delivery. The health system is called University health system (UHS). This system allows lab tests results, doctor prescription and treatment history of patients records to be kept. The study was conducted at the University of Nairobi Hospital because it has implemented an electronic health system which helped the researcher in finding the attributes that have been used to effect confidentiality, integrity and availability which is of concern to the study. Therefore, the study was to enhance the security of the system through the findings and recommendations. This study was carried out on system developers, System support ICT officers and users who have roles in the University Hospital system (UHS).

1.7 Study limitations.

Due to limitations of funding the researcher carried out the research in the mentioned facility and therefore did not collect data from other hospitals which have implemented E- health systems like the referral hospitals. The research on EMR data from a single institution may not be generalizable to broader populations especially since the patients' demographics are not diverse. The mitigation for this limitation was to Validate findings using external datasets from other institutions, regions, or demographic populations to assess the robustness and applicability of the research outcomes.

1.8 Structure of the thesis

This thesis was organized into five chapters. Chapter One served as the introduction, providing a summary of the thesis along with an overview of the expectations and the necessity for the study. Chapter Two was dedicated to the literature review, summarizing existing research and literature relevant to the topic under investigation.

Chapter Three outlined the methodology for the study, detailing the approach the researcher adopted to achieve the study objectives. Chapter Four presented the findings and analysis, showcasing the data collected and its interpretation. Finally, Chapter Five concludes the thesis with a discussion of the results, drawing conclusions and offering recommendations based on the findings. This structured arrangement allowed for a clear progression of ideas and supports a comprehensive understanding of the research undertaken.

CHAPTER TWO

2. LITERATURE REVIEW

2.1 Introduction

This chapter provides a summary of the literature relevant to the study, organized into three key segments: theoretical literature, empirical literature, and a recap of the findings. The theoretical literature lays the foundational concepts and frameworks that underpin the research, offering insights into established theories and models in the field. The empirical literature examined previous research studies, highlighting their findings, methodologies, and contributions to understanding the topic. Finally, the recap of literature synthesized the key points from both the theoretical and empirical segments, drawing connections and identifying gaps that the current study aims to address. This comprehensive review served to contextualize the research within the existing body of knowledge and underscores its significance.

2.2 Theoretical Framework

This section looked at the various theories that were used to inform the study on security features of an E- health system. The study was founded on two theories, the CIA triad in electronic medical records and the Integrated Systems theory. Specifically, literatures pertaining to health system information security in health care systems was reviewed.

2.2.1 CIA Triad in Electronic Medical Record Systems

The Confidentiality, Integrity, and Availability (CIA) Triad is a fundamental model for information security, providing a structured framework essential for protecting electronic medical records (EMRs) in healthcare. With the increasing digitalization of healthcare, EMRs store sensitive patient information, including personal details, clinical notes, test results, and other critical data, which must be securely maintained to ensure patient privacy, regulatory compliance, and effective healthcare delivery (Chen et al., 2020). Applying the CIA Triad to EMRs addresses these security concerns by protecting against unauthorized access, ensuring data accuracy, and keeping systems available to healthcare providers when needed.

2.2.1.1 Confidentiality in EMRs

Confidentiality is the first principle of the CIA Triad and is essential in protecting patient information from unauthorized access and disclosure. Safeguarding confidentiality ensures that only authorized users, such as healthcare providers, can view sensitive patient information (Gostin et al., 2018). In EMR systems, confidentiality measures include role-based access control, multi-factor authentication, and data encryption, which collectively help prevent unauthorized access by limiting data exposure (Zhou et al., 2019). Practically, many hospitals implement role-based access control in their EMR systems, granting healthcare providers access only to information pertinent to their roles. Additionally, encryption protects both data at rest and in transit, helping ensure that even if an unauthorized user intercepts data, it remains unreadable (Shaikh & Sasikala, 2019).

2.2.1.2 Integrity in EMRs

Integrity ensures that patient information within EMRs remains accurate, consistent, and free from unauthorized alteration. This principle is critical in healthcare, where clinicians rely on accurate data for decision-making and patient care (McCarthy et al., 2020). Integrity in EMRs is supported through data validation, audit logging, and cryptographic hashing, all of which help detect and prevent unauthorized modifications to sensitive data (Chen et al., 2020). Practically, In EMR systems, each patient record update is logged, with metadata indicating the user, timestamp, and description of the change. This audit trail provides accountability and helps prevent accidental or malicious data tampering, as any discrepancies can be traced back to their source.

2.2.1.3 Availability in EMRs

Availability is crucial for EMRs, ensuring that patient data is accessible to authorized users when needed. This principle is especially important in healthcare, where clinicians must have timely access to information to deliver effective patient care (O'Connor et al., 2019). Availability is ensured through measures like redundant storage, disaster recovery planning, and regular system maintenance, all of which help prevent system downtime and ensure data is accessible during emergencies (Shaikh & Sasikala, 2019). Practically, hospitals often use cloud-based storage solutions to replicate EMRs across multiple servers and maintain data availability during hardware failures or cyberattacks. In the event of a natural disaster or data breach, backup and recovery protocols ensure that EMRs remain accessible to healthcare providers.

In summary, A CIA-focused approach to EMR security supports compliance with regulations like HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) and fosters patient trust by upholding privacy and data integrity (Zhou et al., 2019). Implementing the triad supports a comprehensive approach to data security, improving patient safety, protecting sensitive information, and fostering trust between healthcare providers and patients. By adhering to CIA principles, healthcare organizations can create secure EMR systems that meet regulatory standards and reduce the risk of breaches. This theory provides a thorough analysis of the CIA Triad within the EMR context, emphasizing the practical application of each principle in ensuring robust security for patient data.

2.2.2 The integrated systems theory

This theory was proposed by Hong et al (2003), as an interdisciplinary theory dealing with any structure of nature, culture, and multiple empirical disciplines, as well as a paradigm with which a phenomenon can be studied from a systematic perspective (Capra, 1997). Integrated System Theory entails enforcement of information security policies, management and assessment of risks, information Auditing and internal controls. Consequently, information security is covered comprehensively in terms of many aspects by integrated system theory. It describes organizational actions in terms of information security management and techniques, as well as including alternatives.

To fully comprehend information security management, explain information security management techniques, and anticipate management outcomes, integrated systems theory is crucial for the study.

Consequently, the theory offers a solid foundation for evaluating the level of information security controls implemented at the University of Nairobi hospital. Internal control is the prevention, detection, and correlation of system-related activities to prevent unauthorized and illegal access.

Controls can also be referred to as administrative, operational, and technical measures that safeguard the system's availability, integrity, and confidentiality.

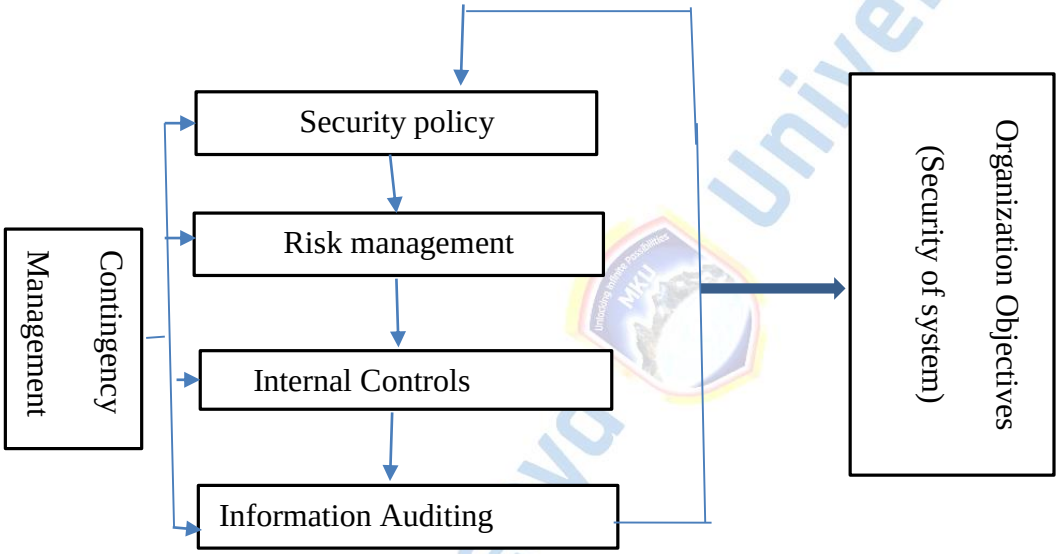


Figure 2: Integrated system Theory (Adapted from Hong et al. 2003)

The nature of this theory makes it difficult to adapt to highly dynamic surroundings, and it also takes a top-down approach that may not be consistent with reality.

We needed to consider M-health as a service delivery system; as argued above in Chapter 2, Integrated System Theory entails enforcement of information security policies, management and assessment of risks, information Auditing and internal controls. Consequently, information security

is covered comprehensively in terms of many aspects by integrated system theory. It describes organizational actions in terms of information security management and techniques, as well as including alternatives. The relevance of the theory in the management of M-health services is deficient in the fact that the theory fails to holistically look at the overall IT infrastructure holistically but instead lays its overall emphasis on information security management.

The big question that this research needed to ask is therefore, how would a holistic integrated information security delivery system look like? What are the optimal IT infrastructure and what security principles would govern the measures that would be put in place to guarantee the security of services for which the system is built?

According to IBM, IT infrastructure configurations vary based on organizational requirements and objectives, however some objectives apply to all businesses. Business high-performance storage, a low-latency network, security, an efficient wide area network (WAN), virtualization, and zero downtime are all features of the ideal infrastructure. This means that to guarantee the security of services supported by these systems, vulnerabilities to each of the components of these systems must be adequately analyzed and addressed.

The security infrastructure of these systems must be designed to regulate data availability and control information access, safeguarding a company from hacks and breaches while maintaining customer trust, regardless of where the data is stored. Wide Area Networks (WANs) must prioritize network traffic and dynamically adjust bandwidth allocation for specific applications as needed to maintain optimal performance. Virtualization technology plays a crucial role in enhancing system uptime,

improving disaster recovery capabilities, conserving energy, and enabling quicker server provisioning.

Furthermore, minimizing downtime is a strategic priority, aiming to reduce system outages and disruptions to business operations, thereby keeping costs low and maximizing earnings.

Given these requirements, it is necessary to divide the security of M-health services into two distinct categories:

1. **Information Security:** This focuses on the core principles of confidentiality, availability, and integrity, ensuring that patient data is protected from unauthorized access and alterations.
2. **MHI Security (M-health Infrastructure Security):** This encompasses the security of the entire M-health infrastructure, including enterprise servers, data storage servers, mainframes, mobile devices, software, and operating systems.

Moreover, a comprehensive approach to secure M-health services must consider that any effective service delivery strategy is comprised of five key components, as outlined by IBM (2016):

1. Service level management
2. Financial management for IT services
3. Capacity management
4. Availability management
5. IT service continuity management

Therefore, any effective M-health system must integrate all these functionalities and requirements into its operations, ensuring a holistic and secure approach to service delivery.

IST in Healthcare Systems

The application of IST in healthcare, particularly in EMR systems, involves examining how different components—such as patient data repositories, decision support systems, and communication networks—interact to support clinical and administrative functions. According to Tan and Payton (2010), IST can help identify inefficiencies and bottlenecks in EMR systems, leading to improved patient care and operational efficiency.

Benefits of IST in EMR Systems

Applying Information Systems Technology (IST) to Electronic Medical Records (EMR) systems offers numerous advantages that significantly enhance healthcare delivery.

1. **Enhanced Interoperability:** IST fosters the integration of diverse health information systems, enabling seamless data exchange and communication across different healthcare providers. This interconnectedness ensures that patient information flows smoothly between various entities, improving coordination of care and reducing the risk of errors (Brailer, 2005).
2. **Improved Data Quality and Accessibility:** By integrating data from various sources, IST ensures that clinicians have access to accurate and up-to-date information. This accessibility is crucial for informed decision-making, ultimately leading to better patient outcomes. The

availability of reliable data supports evidence-based practices and reduces the likelihood of misdiagnosis or treatment errors (Blumenthal, 2010).

3. **Optimized Workflows:** IST plays a vital role in streamlining both clinical and administrative workflows within healthcare settings. By reducing redundancies and automating routine tasks, IST improves overall system efficiency, allowing healthcare providers to focus more on patient care. This optimization leads to faster service delivery, reduced operational costs, and enhanced patient satisfaction (Kellermann & Jones, 2013).

Challenges and Limitations

Despite its numerous benefits, implementing Information Systems Technology (IST) in Electronic Medical Records (EMR) systems is not without its challenges.

1. **Complexity and Integration:** Achieving seamless integration of disparate health information systems requires substantial technical and organizational effort. This process often involves the development and adoption of standardized protocols and interfaces to ensure compatibility and interoperability across various platforms. The complexity of integrating multiple systems, each with its own unique architecture and data formats, can be a significant barrier to successful implementation (Adler-Milstein & Jha, 2014).
2. **Data Security and Privacy:** Ensuring the security and privacy of patient data within an integrated IST framework is a critical concern. As EMR systems become more interconnected, they become increasingly vulnerable to security breaches and unauthorized access. Addressing these risks requires the implementation of robust security policies and advanced

technologies designed to protect sensitive patient information from potential threats. Balancing the need for data accessibility with stringent privacy safeguards is a complex challenge that healthcare organizations must navigate carefully (Goldstein et al., 2007).

2.3 ICT and Healthcare systems

Patient Care Information Systems (PCIS) deployment in healthcare organizations has not been successful. This has been so because of several challenges that may be faced when the systems are being implemented or thereafter (Berg, 2001). Healthcare Information and Communication Technologies (ICT) are complex operational technologies whose applications, purposes, disadvantages, and ramifications are not well defined, nor are the advantages of usage guaranteed. However, there are some compelling theories about how IT can be used in healthcare to increase efficiency, consistency, and connectivity to promote acceptance and guide effective deployment of e-healthcare systems. ICT use ideas are discussed among a group of partners that include medical practitioners, representatives of healthcare organizations, legislative and regulatory authorities, as well as ICT suppliers and consultants. These interactions between a group and systems form and decide the consequences of healthcare ICT technologies. As a result, understanding the social development and interpretive mechanisms by which healthcare ICT technologies are created and shared is important for forecasting consequences of ICT implementation and informing policymakers of the threats presented to patient information contained within these digital networks.

Information security.

Information systems (IS) are highly depended on by organizations. Consequently, these firms employ technical controls to lessen information security risks (Gundu & Flowerday, 2013).

Risk identification.

This refers to the process where potential risks of a project and their characteristics are listed. The results are usually recorded in a risk register.

Risk Management.

Risk refers to the possibility of something adverse happening. Risk management is therefore about transforming organizational culture to accept risk and facilitate risk discussion when doing business activities or making any strategic investment on various projects.

Risk Mitigation

It is a strategy in preparation for and lessening the effects of threats faced by a system.

2.4 Existing frameworks for M-Health Systems.

There is research that have been done on the frameworks for M-health and have been published in various referred journals as discussed below.

2.4.1 A framework for assessing M-Health challenges in South Africa.

A qualitative study conducted in South Africa examined the benefits and challenges of implementing M-health in community-based health services, focusing on four key system dimensions: government stewardship, organizational factors, technological aspects, and financial considerations.

The study highlighted several promising factors for the effective adoption of M-health in South Africa. One of the most significant advantages is the widespread use of cell phones, which provides a strong foundation for M-health initiatives. Additionally, the country benefits from a positive policy framework that supports M-health development, as well as a well-developed ICT industry. The successful implementation of M-health in various community-based health programs further underscores its potential to improve healthcare delivery.

However, the study also identified several challenges that could hinder the full realization of M-health's potential. One of the primary issues is the existing corporate culture within the healthcare system, which may not be fully conducive to the adoption of new technologies. There is also a gap in the ability to use health knowledge effectively for management purposes, as well as limited access to and use of ICT in primary health care settings.

From a technical perspective, the complexities of ensuring interoperability and the convergence of different information systems present significant challenges. Safeguarding information security is another critical concern, as M-health systems must protect sensitive patient data in an increasingly digital environment.

Finally, the study pointed out the issue of financing, particularly the challenge of securing sufficient funds for large-scale M-health implementation in a resource-constrained environment. This financial

barrier could limit the scalability and sustainability of M-health initiatives, despite their potential benefits.

The framework that was developed is as shown in the figure below.

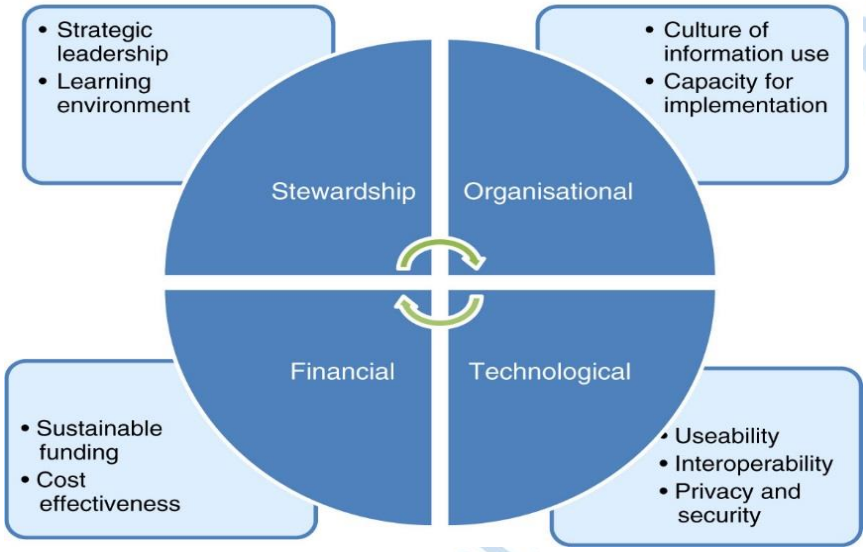


Figure 3:A framework for assessing M-Health challenges in South Africa (Leon et al, 2012)

The figure illustrates four key health system dimensions that must be considered when evaluating the complexities of scaling up M-health from a health systems perspective. These dimensions include government stewardship, organizational factors, technological aspects, and financial considerations. Each of these areas plays a crucial role in determining the success and sustainability of M-health initiatives as they expand.

However, a significant research gap was identified in the study: the security of M-health systems was not adequately addressed. While the study provided valuable insights into the various challenges and opportunities associated with scaling up M-health, it overlooked the critical issue of ensuring that these systems are secure. In an era where digital health technologies are becoming increasingly integrated into healthcare delivery, the omission of security considerations is a notable shortcoming. Addressing this gap is essential for protecting patient data, maintaining trust in M-health solutions, and ensuring the long-term viability of these technologies within the health system.

2.4.2 M-Health decision making framework for community-based services

Maranda (2016), the researcher encompassed additional security procedures using encryption, integrity of the data and the security keys. In the encryption perspective, encrypted data was sent to the server. The researcher used built-in libraries for encryption of string data. The messages were transferred in XML format to the server

Maranda (2016) implemented integrity of the data using Digital signatures. The Digital signature ensured that the message that was sent was exactly what was received. The signature depended on the encryption which assured authentication.

The Digital signature solely relied on a private key algorithm. This meant that the message owner was the only one who knew it but the public key was known. The researcher used checksum algorithms and a checksum function to transform the input and produced a numerical output of smaller size.

He suggested the use of security keys. In this case he used 128bit strings which were delivered to the server before requesting sensitive data. The security keys were encoded with chosen cryptographic algorithm and were unified with entire application but quite independent from the device.

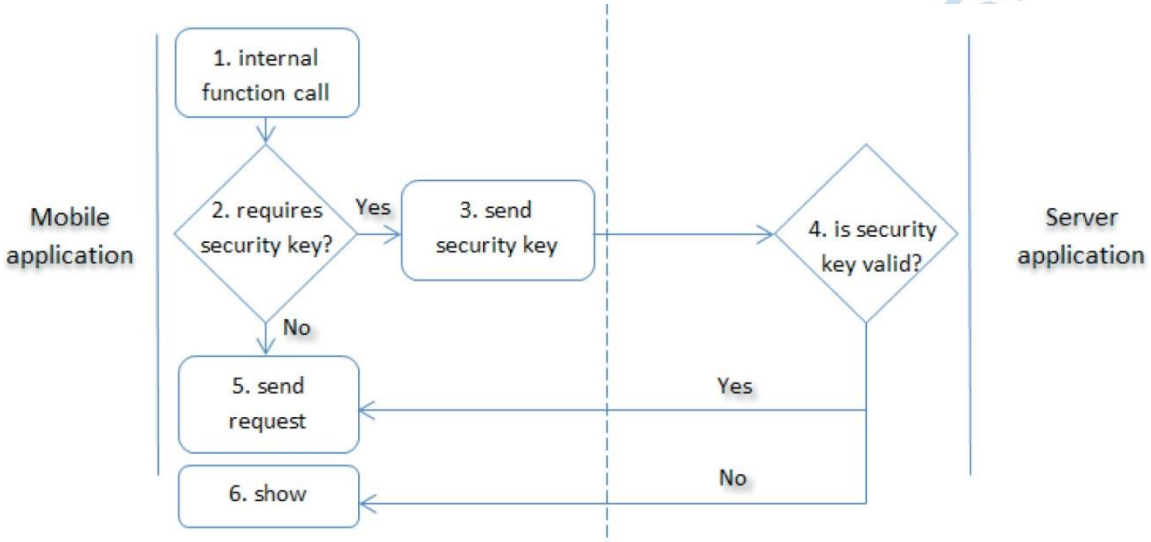


Figure 4: Data transfer using encryption and digital signatures. (Maranda,2016)

In this study, the researcher introduced three core components that must be considered while developing and deploying mobile applications. These components were: data transfer, storage, and access. All these components must be viewed as equally important all through all phases of development. The Secure Development Strategy detailed the assumptions and frameworks that ought to be enforced within the application context to provide mobile protection. The most important feature of Secure Development Strategy is that it embraced all crucial aspects by describing the concepts and grouping them. The geo-location and ADID (Application Device Identifier) for data access, the

encryption of sensitive data in database files, and the encryption of requests transmitted over the internet with digital signatures and security keys were not addressed by the researcher in this study. The Secure Development Strategy's objectives were to limit the number of potential risk points in the program rather than to completely protect it from assault by preventing potential attackers from encrypting important data. With the use of a developed security architecture called iSec, the Secure Development Strategy's pillars were really put into practice.

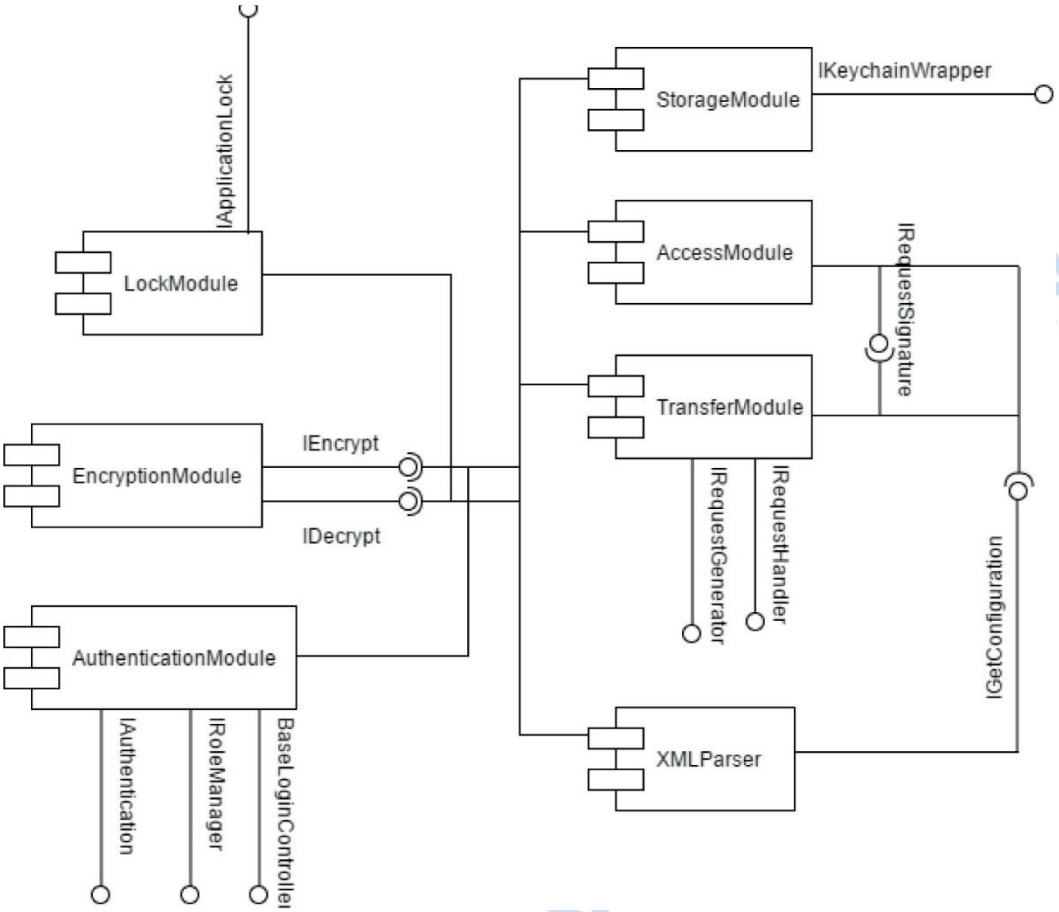


Figure 5: Components of the iSec framework. (Maranda, 2016).

The study's research gap was that the privacy of patient records was not examined.

2.4.3 Mobile Application Security System Framework.

For mobile application networks, Floyd (2006) developed creative layering of security mechanisms that offered a dispersed security solution. Code signature variation, remote hashing, a mobile

application generator, application time to live, resident monitor applications, distributed application monitoring, code obfuscation, and hashing algorithms were all provided by the researcher in a way that maximizes benefits while minimizing overhead. The researcher offered a distributed method that could keep safeguarding even if hosts and programs were deleted, corrupted, or destroyed. The integrity and security of the application system were strengthened by the security measures described in this study.

The limitation of this research is that the researcher didn't address methods for detecting and preventing denial of service (DoS) attacks and secured interprogram communications. Diverse application kinds must collaborate through interprogram communications to carry out an essential task.

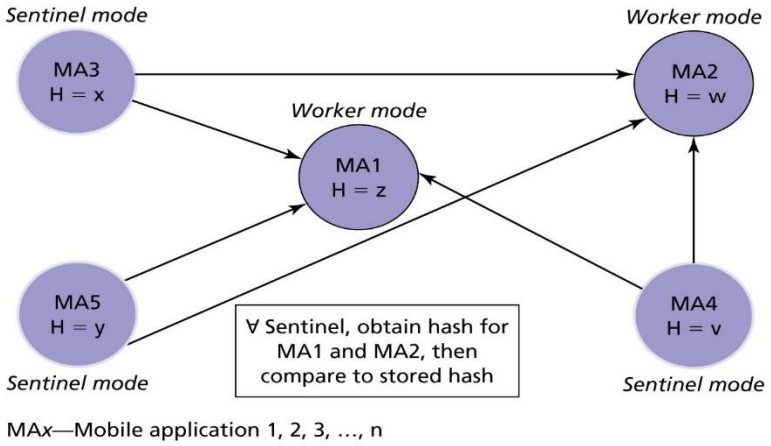


Figure 6: Analyzed hashes obtained for the conflicting parties. (Floyd, 2006))

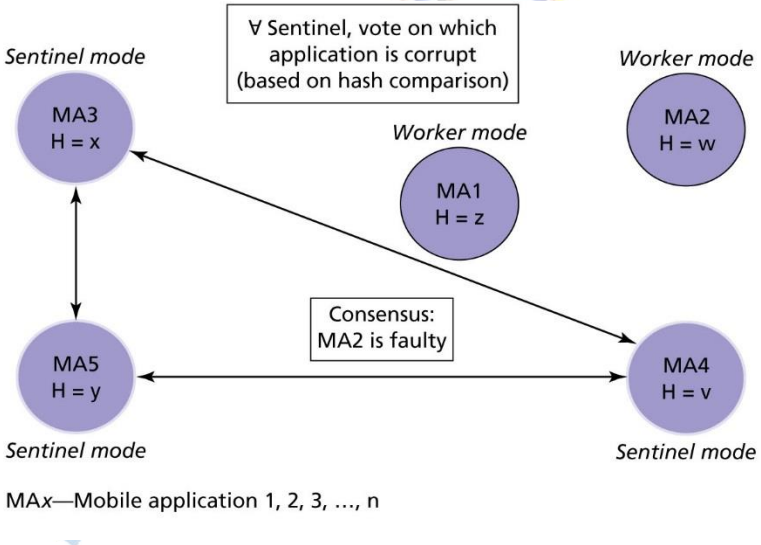


Figure 7: Corrupt application identified by consensus vote (Floyd, 2006)

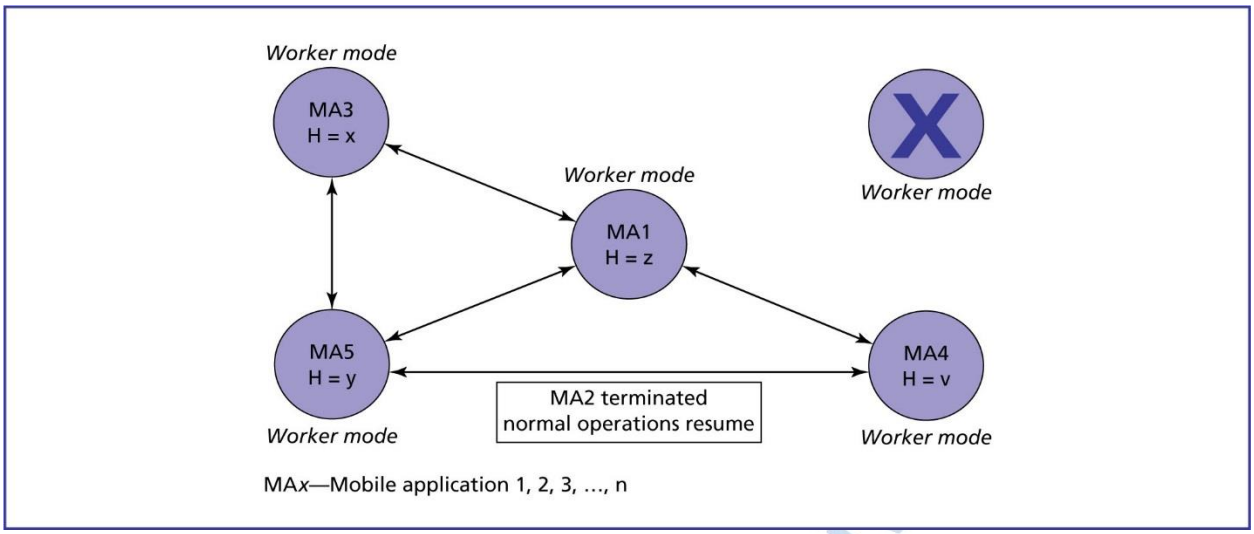


Figure 8: Termination of corrupt application from the network. (Floyd, 2006)

2.4.4 A framework to improve mobile banking security.

In this case, the researcher recommended providing banking customers with a smartphone device so they could safely access their business or personal accounts from any location at any time.

To resolve these security issues, a confident negotiation approach was suggested in this report. As the underlying protocol, trust negotiation was paired with Transport Layer Security (TLS). This technological mix aimed to improve the current security of M-banking applications.

The proposed framework verified the requesters and their devices. These gave users the chance to register their mobile devices and provided a mechanism for financial organizations to confirm that the device was being used. By automating the authentication process, this strategy improved two factor authentication.

The limitation of this study is that it did not factor in the location verification method to the m-banking system.

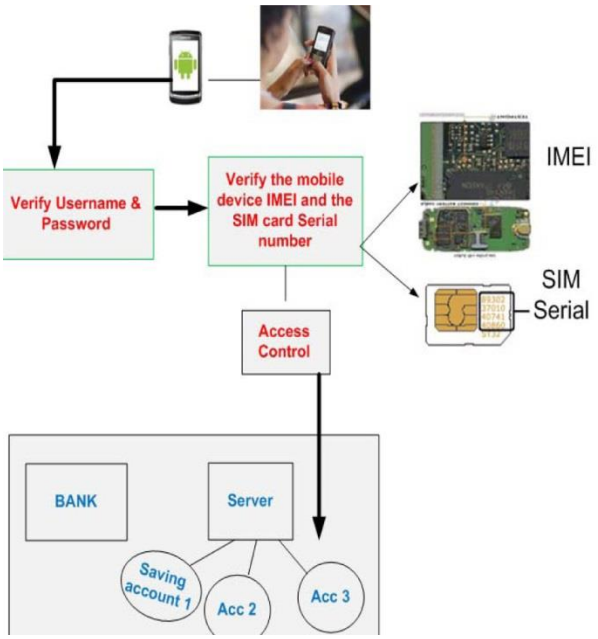


Figure 9: Secure M-banking model ((Source, Elkhodr (2012))

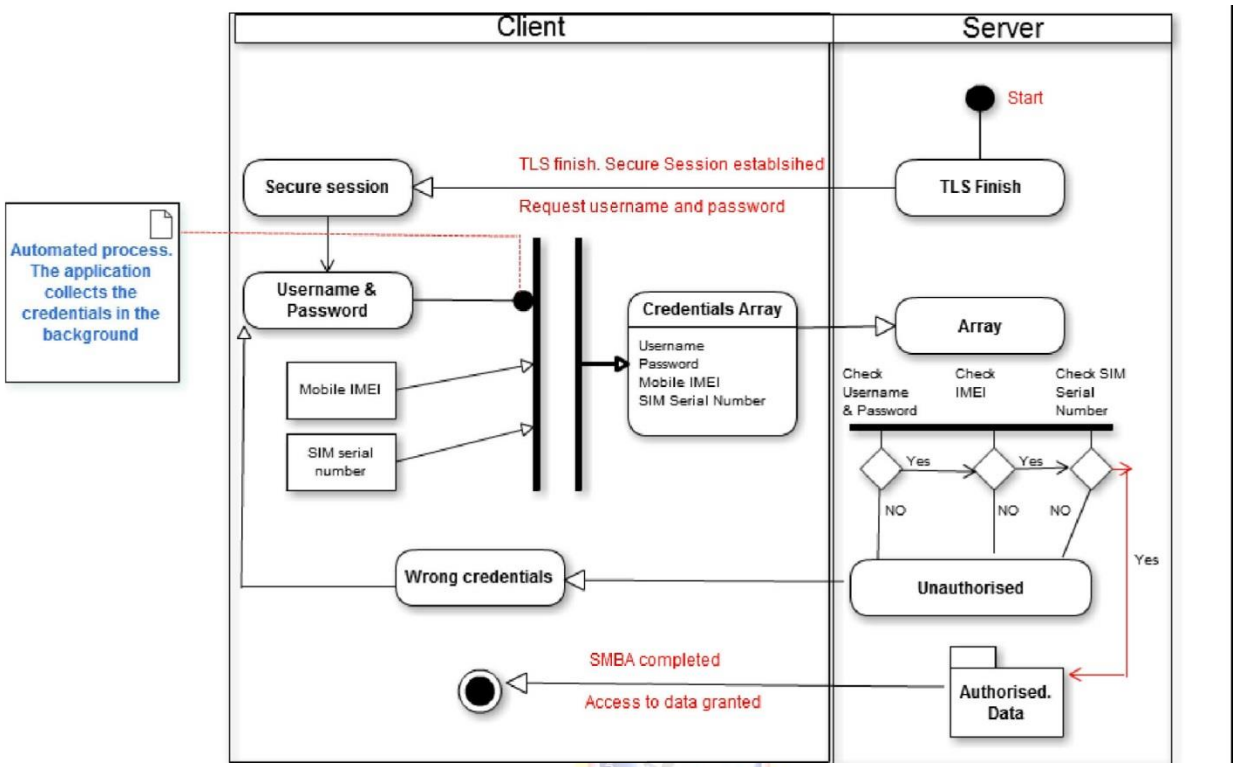


Figure 10: Secure mobile banking approach framework activity diagram. (Elkhodr, 2012)

The researcher did not consider location verification in the mobile banking system.

2.4.5 An Enhanced Mobile Health Applications Cloud Computing Framework

The researcher described the difficulties that mobiles encounter when providing Secure Multimedia-based Health Services due to computation and power supply constraints in this report.

In this case, the researcher postulates that mobile devices are not able to perform complex multimedia and security Algorithms because they run on small batteries and have inadequate computational capacity, as a result, researcher devised a cloud computing platform to support mobile devices while

running heavier multimedia and encryption algorithms in the distribution of mobile health services. In this study, the suggested framework makes use of a cloud computing protocol management approach to offer mobile devices security as a service (SaaS) and multimedia sensor data processing. The researcher in this study hypothesized that security and multimedia operations may be carried out in the cloud, enabling mobile health service providers to subscribe and expand the features of their mobile health applications beyond the limitations of currently accessible mobile devices.

In this research, the security of mobile health systems data was not addressed by the researcher hence the need to carry out more research on this topic.

The initials of the diagram.

NI- is a non-intrusive sensor that is used to gather the required sensor signals, which are then fed to an embedded digital signal processor (DSP) in a mobile device.

SIPS-is the session initiation protocol signaling

SIP-EP-is the session initiation protocol event packet, this connects the IMS client to the call session control functions (CSFC).

The CSFCs are SIP proxy servers, supporting IMS signaling and session control functions.

XDMS- is the database management system which controls and organizes data created by the health monitoring services.

The Application server hosts the ongoing mobile service and sends and receives data from the IMS client. The application server also functions as a branch of the Home Subscriber Server (HSS), which is the primary repository of mobile-related user data. The IMS system monitors acts as the recipient and interpreter of the sensed physiological information and therefore relays back the necessary decision and action to be taken.

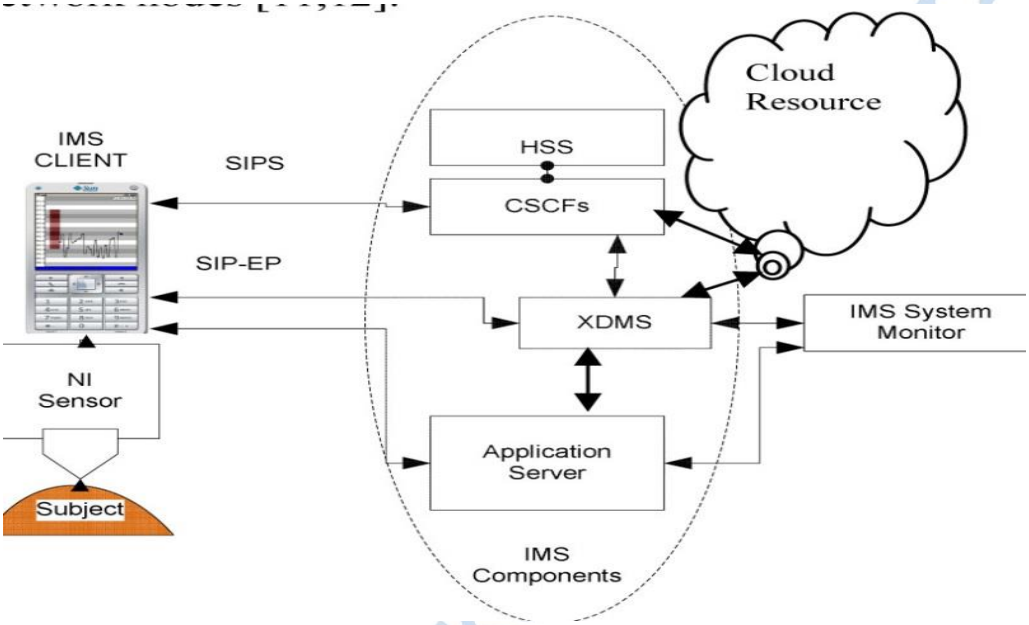


Figure 11: A framework of IP multimedia subsystem standard –based mobile health monitoring with cloud support. (Nkosi& Mekuria, 2010)

2.4.6 Secure mobile data collection system framework.

Gejibo (2015) developed a secure mobile data collection system framework with a set of modular security features that were built to meet MDCS standards and design criteria. The framework included simple interaction interfaces. The framework was created to be flexible, scalable, and adaptable to

various MDCS security settings while simultaneously being secure by default. The framework's primary goal was to offer an all-encompassing safe solution for user identification, secure mobile and cloud storage, and secure communication.

Authenticator: a security module that dealt with account recovery, remote server authentication, and user authentication on mobile devices. With a default concrete implementation, it offered authentication services through straightforward interfaces.

This module received the user authentication delegation from the MDCS client. As a result, whenever an attempt was made to access the MDCS (mobile data collection systems) client, the Authenticator module was invoked. The Authenticator is adaptable and may be set up to offer further capabilities like single sign-on and device authentication. The requirement that a phone may be shared by several collectors who should not have access to each other's acquired data was the major justification for the module's existence.

2. Secure Storage: Security module in charge of managing and protecting the mobile device's MDCS application resources. With a default concrete implementation that handles encryption, decryption, cleaning up leftover data once the user logs out, and a recovery strategy in case the application crashes or the battery runs out, the secure storage is available via straightforward APIs.

3. Secure Communication: is a security component in charge of creating a secure tunnel between the client and the server. A popular protocol for protecting HTTP messages is Hypertext Transfer Protocol Secure (HTTPS).

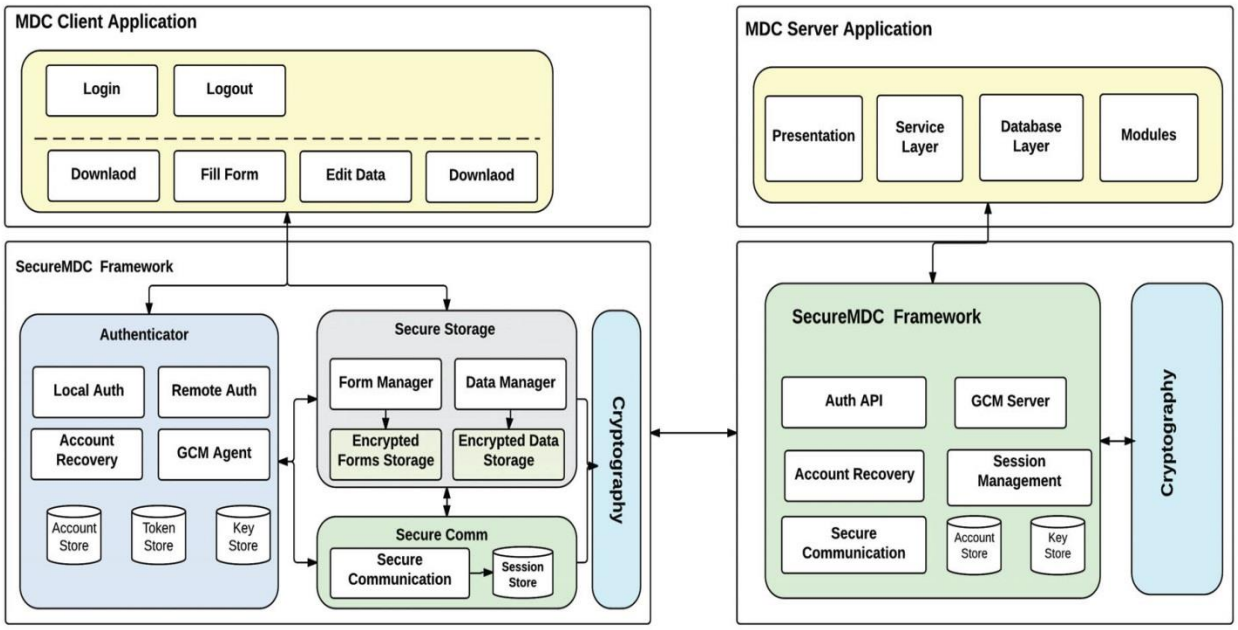


Figure 12:showing the modules and the explanation (Gejibo,2015)

2.4.7 SecourHealth Framework.

Simplicio et al. (2015) in his SecourHealth, developed a minimal security framework with a focus on very sensitive data collection systems. In this he identified various pillars which included:

I. Lack of connectivity and tolerance delays- Users were able to function offline when necessary and authenticate themselves on any device they had previously registered.

II. Loss or theft device protection- When a device is stolen while a legitimate user's session is still active, this module has a method that restricts the attacker's ability to receive information from the server.

III. Data transfer between a mobile device and server in a secure manner- In this module, even in the absence of an underlying secure connection, all data sent between a server and a mobile device was encrypted and authorized.

By incorporating this security framework into the GeoHealth system and the Android-based "Family Health Program" application, which were both used by the government to collect health data in Sao Paulo city, Marcos (2015) put this security architecture into action. In this study, the researcher did not identify potential vulnerabilities in data security and privacy within the framework, especially with increased use of digital health records.

2.5 Conceptual framework

Figure 12 shows the conceptual framework for this research. In order to assess your electronic health record security, credibility, and availability requirements, you must first thoroughly consider your practice's health IT climate. This could include the technology your profession uses for both therapeutic and institutional purposes, as well as when and how those technologies are physically used and located within your practice. Consider the circumstances that could result in unwanted entry, use, leak, interruption, alteration, or loss of electronic health records as you assess the health IT climate. These circumstances are likely to be specific to the practice and can take the form of technology problems (e.g., a lack of securely installed computing equipment), procedural issues (e.g., a lack of a security incident management plan), or staff issues (e.g., lack of comprehensive information security training).

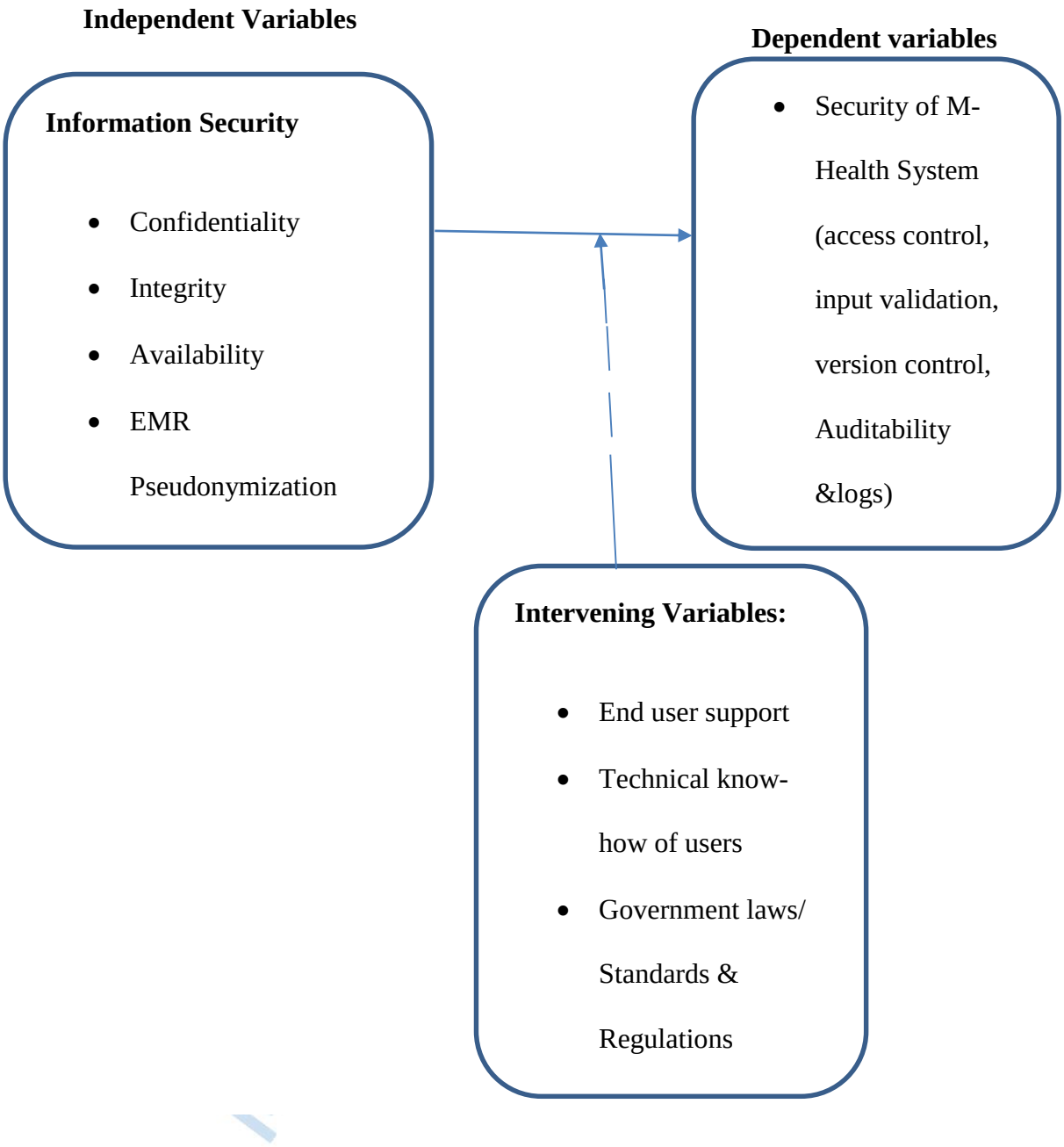


Figure 13: Conceptual framework, Researcher 2024.

2.5.1 Confidentiality

The security of information contained inside networks from unwanted or unintended access is referred to as confidentiality.

“Privacy is an individual's right to choose when, how, and to what degree knowledge about them is transmitted to others” (Brands, 2003, pp2). Privacy involves the right of the individual to be left alone , to withdraw from the influence of his environment (Innab, 2018).Additionally confidentiality relates to disclosure or nondisclosure of information.

Patients agree that with their permission their medical data can be shared with other institutions such as insurance companies to facilitate the payment of their dues. Therefore, the patients only understand that the shared individual medical data can only be used for the intended purpose.

Furthermore, outside the hospital, patients had expectations that individuals were not given access to confidential information or institutions not permitted to keep such content. The content's genuine users won't abuse this access for uses other than those for which it was intended in the first place.

Ensuring confidentiality in Electronic Medical Records (EMR) is essential for safeguarding patient privacy and upholding trust in the healthcare system. The following are essential elements of confidentiality in Electronic Medical Records (EMR):

1. **Legal and regulatory frameworks**

HIPAA, which stands for Health Insurance Portability and Accountability Act, establishes the benchmark for safeguarding confidential patient data in the United States. It requires healthcare providers, insurance organizations, and other entities managing EMRs to establish measures to protect the privacy, accuracy, and accessibility of electronic health information.

The General Data Protection Regulation (GDPR) is a set of regulations in the European Union that safeguards personal data and guarantees privacy for individuals, including electronic medical records (EMRs). Healthcare providers must get explicit consent from patients before processing their data and must adhere to strict criteria on data handling.

2. **Measures to ensure technical security.**

Data encryption is a security measure that protects critical EMR data from unwanted access, both when it is being transferred and when it is stored.

Implementing role-based access restrictions in the EMR system guarantees that only authorized individuals can access specific information. This encompasses security measures such as distinct user identifiers, robust passwords, and biometric authentication.

Audit trails are essential for preserving a record of activities and monitoring the use of electronic medical records (EMRs). They play a crucial role in identifying and examining instances of unauthorized access or security breaches. It is crucial to regularly monitor these logs.

3. **Measures to protect and manage administrative processes**.

Creating and implementing thorough policies and procedures for the access and management of Electronic Medical Records (EMRs) is crucial for maintaining confidentiality. This encompasses instructions for the exchange of data, the duration for which it is kept, and the actions taken in response to incidents.

Training and awareness: It is crucial to provide healthcare professionals with regular training on the significance of confidentiality, data protection legislation, and the most effective methods for handling electronic medical records (EMRs). Implementing awareness campaigns can effectively mitigate inadvertent breaches caused by human mistake.

Regularly conducting risk assessments to detect potential vulnerabilities in EMR systems and implementing strategies to reduce these risks is crucial for ensuring confidentiality.

4. **Rights of the Patient.**

Consent Management: Patients should possess authority over determining who individuals are granted permission to access their medical information. Enabling the implementation of systems that enable patients to provide or revoke authorization for data sharing guarantees their autonomy and privacy.

Record Access: Patients possess the entitlement to retrieve their medical records. EMR systems should enable this process while ensuring that access does not jeopardize confidentiality.

5. **Response to an Incident.**

Data Breach Notification: Promptly notifying impacted patients and necessary authorities is crucial in the event of a data breach. This is a mandatory obligation that must be fulfilled in accordance with both the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR).

Implementing corrective actions to rectify the underlying cause of a breach and proactively prevent future incidents is imperative. This may entail implementing enhanced security protocols, providing staff with additional training, or revising existing policies.

6. **Compatibility and Exchange of Information.**

Secure Data Exchange is crucial for ensuring confidentiality in the healthcare industry. It involves the use of established protocols such as HL7 and FHIR to ensure that data transferred across different healthcare providers and systems is done safely. When utilizing third-party suppliers for EMR-related services such as cloud storage and data analytics, it is crucial to verify their adherence to confidentiality standards and the presence of strong security protocols.

7. **Advancing Technologies.**

The utilization of AI and machine learning in the healthcare sector has a multitude of advantages, while also posing potential hazards to the preservation of confidentiality. It is imperative to ensure that these technologies are created and implemented with robust data protection procedures.

Blockchain technology is being investigated for its ability to improve the confidentiality of electronic medical records (EMR) by creating secure and unchangeable information. Nevertheless, the practical application and capacity to expand the system still pose difficulties.

By attending to these factors, healthcare organizations can guarantee the confidentiality of electronic medical records (EMRs), thus safeguarding patient privacy and upholding faith in digital healthcare systems.

2.5.2 Integrity

Integrity in the context of electronic health records refers to the property that ensures the data has not been tampered with or lost in an improper way. It emphasizes the accuracy and consistency of the information stored about an individual, entity, or event—in this case, the patient (Charitoudi & Blyth, 2013). Integrity of data encompasses documentation accuracy throughout the entire health record. It entails patient identification, information governance, record correction and validation of authorship. Additionally, the accuracy of the data provided at the time of capture has a significant impact on the quality of the data in the EHR.

The quality of a patient's healthcare may be significantly impacted by inaccurate health information. As health information becomes more computerized and the extent of organizational interchange of health information expands into Health Information Exchanges, maintaining the accuracy and completeness of health data is essential (HIEs) (Kellerman & Spencer, 2013).

According to Lucas (2013), patient identity integrity is defined as the accuracy, reliability, and completeness of the demographic information associated with a specific patient. Integrity in Electronic Medical Records (EMR) guarantees the accuracy, consistency, and reliability of the data throughout its lifespan. Ensuring the accuracy and reliability of electronic medical records (EMRs) is essential for delivering excellent patient care and facilitating informed clinical decision-making. Here are crucial elements to guaranteeing integrity in Electronic Medical Records (EMRs):

1. **Precision and Uniformity of Data.**

Validation Checks: Incorporating validation checks during data entering to proactively prevent errors. This encompasses validations for data types, formats, and ranges.

2. **Standardization**:

The utilization of standardized terminology and coding systems, such as ICD-10 and SNOMED CT, guarantees that data remains consistent and can be compared across various systems and timeframes. Regular Audits: Performing periodic examinations and assessments of EMR data to detect and rectify any inaccuracies or discrepancies.

3. **Measures to ensure technical security**

Data encryption is a process that guarantees the integrity of data by preventing unauthorized modification or access during its transport or storage. This ensures the integrity of the data by preventing unauthorized modifications.

4. **Access restrictions:**

Enforcing robust access restrictions to guarantee that only authorized personnel have the ability to edit EMR data. Role-based access control (RBAC) limits access by enforcing restrictions depending on the user's designated role.

5. **Audit Trails**

Maintaining comprehensive records of every instance of accessing and altering EMR data. This facilitates the process of monitoring modifications and detecting unauthorized changes.

Data backup and recovery is the process of creating copies of data and restoring it in the event of data loss or system failure.

Regular backups involve the routine process of creating copies of EMR data to mitigate the risk of data loss caused by system malfunctions or unforeseen catastrophic events. It is important to securely store and regularly test these backups.

Disaster Recovery Plans: Implementing a thorough disaster recovery plan to guarantee prompt recovery of data and services in the event of a system breakdown or breach.

4. Ensuring the dependability and duplication of the system.

Fault-tolerant systems are designed to ensure the continuous operation of EMR systems even in the presence of hardware or software failures. This involves the utilization of duplicate systems and components.

Regular maintenance involves conducting routine upgrades and maintenance tasks on EMR systems to guarantee their optimal performance and security. This measure serves to mitigate system malfunctions and safeguard against data integrity issues.

5. Standards for compatibility and communication across different systems

Utilizing standardized protocols, such as HL7 and FHIR, guarantees the reliable and consistent movement of data between various systems.

Data Mapping: Ensuring accurate data mapping throughout the integration of data from many sources to uphold consistency and integrity.

6. User Education and Consciousness

Effective instruction: Offering thorough instruction to users on correct data input procedures and the significance of maintaining data accuracy. This leads to a decrease in errors and enhances the quality of data.

Conducting awareness campaigns to educate employees about potential risks to the integrity of data, such as cyber-attacks and human errors.

7. Adherence and Surveillance

Regulatory Compliance: Ensuring adherence to applicable legislation and standards (such as HIPAA and GDPR) that encompass requirements for preserving data integrity.

Continuous monitoring is the act of implementing a system to constantly observe EMR systems in order to immediately discover and respond to any breaches in their integrity. This encompasses the utilization of automated tools as well as the examination conducted by humans.

8. Advancing Technologies

Blockchain: Utilizing blockchain technology to enhance the integrity of data by creating unchangeable records and providing clear transaction histories.

Artificial Intelligence (AI) is employed to detect trends and anomalies that may suggest data integrity problems, facilitating proactive data quality monitoring.

9. **CDSS stands for Clinical Decision Support Systems.**

Ensuring the accuracy and currency of data input is crucial for the CDSS to give credible recommendations and alerts. Feedback procedures: Establishing procedures for doctors to report inaccuracies in EMR data, which can subsequently undergo review and correction.

Healthcare organizations may guarantee the integrity of EMRs by prioritizing these characteristics, which are crucial for efficient patient care, clinical decision-making, and upholding trust in the healthcare system.

2.5.3 Availability

Availability refers to the characteristic of electronic health information that ensures it can be accessed and utilized by an authorized individual when needed. System availability measures the period during which operations are functional, indicating how frequently the system is operational. This is typically expressed as a ratio of up-time to the sum of up-time and downtime, with various formulaic variations (Ahmed & Mousa, 2016). Up-time and downtime represent distinct conditions: up-time denotes the system's ability to perform its designated duties, while downtime indicates an inability to carry out these tasks (Charitoudi & Blyth, 2013).

When a system is up and running and ready for use, it is said to be available. A system may go offline for a variety of reasons, ranging from scheduled maintenance downtime to catastrophic failure (Innab, 2018). The goal of high availability solutions is to reduce this downtime and/or the amount of time it takes to recover from an outage (Zdravkova, 2015). How much downtime may be permitted will influence the solution's comprehensiveness, complexity, and cost.

On the extreme end of the scale, high availability can literally refer to a disaster response plan that can get an organization back up and running as soon as possible. For small systems, this may be as straightforward as an uninterruptible power source and a strict backup strategy. The peak of consistent availability, exemplified by comprehensive workload-sharing solutions distributed across several sites, is at the other end of the spectrum. There are differing degrees of availability between these two extremes (Nganji & Nggada, 2011). Computing systems availability has been described using various concepts: high availability computing; fault tolerant systems; system redundancy (Lizasoain et al.,

2015). The idea behind all this is to ensure that no matter what happens, users must be able to access the systems for the data and information that they require. In the case of e-health, system failure can be initiated at five levels.

- Mobile device failure (hardware/software)
- Network outrages
- Or server failure (hardware or software)

Wherever any of this happens, it leads to delays in access of the systems or failure by the users to perform the functions for which they are supposed to. Thus, system designers must do their best to develop contingency plans that will ensure continued access of these vital systems.

Electronic Medical Records (EMR) availability guarantees timely access to data, facilitating uninterrupted healthcare provision and optimizing operational effectiveness. Here are fundamental elements to guaranteeing availability in Electronic Medical Records (EMRs):

1. System Redundancy and Reliability.

Redundant Systems: The implementation of duplicate systems and components to eliminate the presence of any singular points of failure. This encompasses the implementation of redundant servers, network routes, and storage devices.

2. High Availability (HA) Architectures: Developing EMR systems with HA architectures, such as clustering and load balancing, to guarantee uninterrupted availability even in situations of high usage or component malfunctions.

3. Measures for recovering from disasters and ensuring uninterrupted business operations.

calamity Recovery Plans (DRP) involve the creation and upkeep of thorough plans to swiftly restore EMR functionality following a calamity. This entails conducting periodic testing and implementing revisions to the Disaster Recovery Plan (DRP). Business Continuity Planning (BCP) refers to the process of establishing strategies and procedures to ensure the uninterrupted functioning of critical processes and activities in the event of an interruption.

3. **Implementation of regular backup procedures and data recovery protocols.**

Regularly scheduling backups of EMR data to prevent any potential loss of data. It is important to safely store backups in multiple locations. Data recovery testing involves regularly assessing the efficacy of data recovery procedures to ensure the prompt and accurate restoration of backups when necessary.

4. **Networking Infrastructure.**

Ensuring the network infrastructure supporting EMR systems is resilient and dependable. This involves utilizing fast, secure networks and ensuring an adequate amount of bandwidth. Network redundancy involves the implementation of several internet service providers (ISPs) and backup network links to prevent interruptions.

5. Measures to ensure the security of computer systems and networks.

Implement robust cybersecurity measures to safeguard against cyber threats, including malware, ransomware, and DDoS attacks, which have the potential to impair the availability of EMR. Security Monitoring: Ongoing surveillance to detect and address potential security breaches and vulnerabilities, employing proactive methods to reduce risks.

6. Routine maintenance and updates

System Maintenance: Regularly scheduling maintenance to ensure that hardware and software components are kept up-to-date and operating efficiently. This encompasses the tasks of managing patches and updating software. Performance Monitoring is the ongoing observation of system performance in order to identify and resolve any issues before they have a negative influence on availability.

User Access Management refers to the process of controlling and regulating the access that users have to a system or network. Role-Based Access Control (RBAC) is implemented to guarantee that users are assigned appropriate access levels, hence preventing unauthorized behaviors that may compromise system availability.

7.Scalable Access Solutions: Ensuring that access control systems can accommodate a growing number of users without any decrease in performance.

8. **Compatibility and Exchange of Information**: Utilizing standardized protocols such as HL7 and FHIR is essential for achieving smooth interoperability between various EMR systems and

healthcare applications. Interoperable Systems: Developing EMR systems with the capability to seamlessly connect with other healthcare systems, enabling streamlined data sharing and minimizing disruptions during transitions or integrations.

9. Cloud Services and Virtualization: Cloud-Based Solutions: Utilizing cloud services for EMRs to take advantage of the superior accessibility, scalability, and disaster recovery capabilities provided by cloud providers. Virtualization involves the utilization of virtualization technologies to enhance flexibility, enabling the swift deployment of supplementary resources and expedited recovery in the event of hardware faults.

10. User Training and Support: Training Programs: Offering extensive training to healthcare personnel to ensure their proficient utilization of the EMR system, hence minimizing errors and inefficiencies that may affect accessibility. Technical Support: Providing comprehensive technical assistance to promptly address and resolve any user concerns, guaranteeing minimal interruption to EMR access.

11. **Advancing Technologies:**

AI and Machine Learning: Employing AI and machine learning to forecast and proactively resolve possible system problems, enhancing performance and availability. Blockchain: Investigating the potential of blockchain technology to offer decentralized and highly accessible data storage solutions.

By attending to these factors, healthcare companies may guarantee the uninterrupted accessibility of EMRs, thus promoting efficient patient care and operational effectiveness.

2.5.4 Pseudonymization.

Pseudonymization is an essential method used in data protection, particularly for safeguarding sensitive data like electronic medical records (EMRs). This method entails substituting identifiable information with pseudonyms, so safeguarding people' privacy while enabling the utilization of data for analysis and research purposes. Presented below is an elaborate summary of many methods used for pseudonymization:

1. The process of tokenization.

Tokenization is the process of replacing sensitive data pieces with a non-sensitive version, known as a token, that lacks any exploitable value. The correlation between the initial data and the token is upheld in a distinct and secure database referred to as a token vault.

Benefits: The original data remains confidential and is never disclosed beyond the secure environment.

Tokens can be created to align with the structure of the initial data, hence maintaining the usability of the data.

Drawbacks: Demands the implementation of a safe system for managing the token vault.

In the event of a breach in the token vault, it is possible to re-identify all tokenized data.

An example of a use case is in the healthcare industry, where patient identifiers such as names or Social Security Numbers can be tokenized. This allows researchers to utilize the data without having access to any identifying information.

2. The process of converting information into a secret code or cipher to prevent unauthorized access.

Encryption is the process of converting data into a coded format that can only be understood by someone who possesses the decryption key. Encryption alone does not constitute pseudonymization. However, provided the key is properly handled and kept separate, encrypted identifiers can act in a similar way.

Benefits: Robust security measures to safeguard confidential information.

Can be seamlessly incorporated into preexisting IT systems.

Drawbacks: Encryption key management is necessary.

Data decryption is necessary to access and utilize data, however this process also brings forth potential security vulnerabilities.

An example of a use case is the encryption of patient IDs in electronic medical records (EMRs), which guarantees that only authorized users with the decryption key can retrieve identifying information.

3. Hashing refers to the process of converting data into a fixed-size value or key that represents the original data.

Hashing is the process of using a mathematical procedure, known as a hash function, to transform data into a string of characters with a set length. This string of letters may seem random. Popular examples of hash functions include SHA-256 and MD5.

Benefits: Hashes are non-reversible, which increases security.

This tool is valuable for confirming the accuracy and completeness of data.

Drawbacks: Hash collisions can arise when distinct inputs yield identical hash values.

Not appropriate for scenarios in which data must be re-identified.

An example of a use case is when patient IDs are hashed, enabling the comparison and matching of records between datasets without revealing the original IDs.

Data masking is a technique used to protect sensitive data by replacing it with fictitious or altered data.

Data Masking is a technique that substitutes genuine data with fabricated yet plausible data. This technique can be either static, meaning it is permanently altered, or dynamic, meaning it is altered on the fly during data retrieval.

Benefits: Preserves the usefulness and authenticity of the data for the purposes of testing and training. Can be customized to accommodate various data formats and application scenarios.

Drawbacks: Elaborate execution.

Not appropriate for situations that necessitate re-identification.

An example of a use case is utilizing masked data in a training environment, which enables developers to manipulate realistic data without revealing genuine patient information.

Perturbation refers to a disturbance or disruption in a system or process.

Perturbation refers to the act of making tiny modifications to data in order to conceal its original values while maintaining its statistical characteristics. Methods encompass the incorporation of noise or the implementation of differential privacy techniques.

Benefits: Strong level of confidentiality and maintains the general data patterns and trends.

Drawbacks: Can impact the precision of the data and the challenge is to implement with optimal efficiency.

An example of a use case is the addition of noise to the age data of patients in a research dataset. This is done to protect the identity of the patients while still ensuring that the dataset remains relevant for statistical analysis.

6. Generation of Artificial Data

Synthetic Data Generation is the process of producing totally fabricated datasets that accurately mimic the statistical characteristics of the original data, while avoiding the use of any real sensitive data.

Benefits: Minimizes the possibility of re-identification.

Can be utilized without any apprehensions regarding privacy.

Drawbacks: Producing high-caliber artificial data can pose difficulties and this data may not accurately capture all the subtle details of the original information.

An example use case is the generation of synthetic patient records for the purpose of training machine learning models in healthcare applications.

7. Anonymization of Data.

Data Anonymization is frequently conflated with pseudonymization; however, it is a more enduring procedure in which data is modified in an irreversible manner to hinder re-identification.

Benefits: Utmost level of data confidentiality and there is no requirement to handle re-identification keys or mappings.

Drawbacks: Irreversible, rendering it inappropriate for situations that necessitate re-identification. Improper execution can diminish the effectiveness of data use.

An example of a use case is the publication of healthcare datasets that have been anonymized for the purpose of public study, while also safeguarding the privacy of patients.

Practical Implementation of Pseudonymization.

To effectively perform pseudonymization, it is necessary to follow many steps:

Evaluate the data: Determine the specific data items that require pseudonymization.

Choose Techniques: Determine the most suitable pseudonymization techniques by considering the inherent characteristics of the data and its intended purpose.

Formulate policies: Establish thorough policies for the management of data, encompassing pseudonymization, re-identification, and access controls.

Implement Technology: Utilize technological solutions to automate the process of pseudonymization and guarantee the secure handling of data.

Training and Awareness: Provide personnel with education regarding the significance of data privacy and the precise methods of pseudonymization being employed.

Conduct regular monitoring and auditing to ensure that pseudonymization techniques are both successful and in compliance with legislation.

Using a pseudonym can aid in safeguarding one's privacy. Through the implementation of pseudonymization, it is possible to safeguard sensitive data while allowing individuals to access less

critical elements. To manage sensitive information, this approach substitutes vital data components with pseudonyms. This strategy restricts quick access to information.

2.5.5 Standards and Regulations

The Health Insurance Portability and Accountability Act (HIPAA)

Any electronic health records system that ensures the privacy and security of patient data must adhere to standards. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the regulation that is most frequently used in the US. Health information is protected by federal law known as HIPAA, which also guarantees that patients can access their own medical records. The people in charge of safeguarding this information now have additional obligations. HIPAA sets security standards that are comprised of four areas as stated by Maiwald (2005). These four sections include technical security services, physical safeguards, technical security mechanisms and finally administrative procedures. The main objective of HIPAA is to keep customers' and employees' personal health information private, secure and confidential. The personal Health information must also be maintained in a manner that ensures high integrity and high availability in the event of an emergency. Another standard in use is the CEN/ISOEN3606-PartIV in Europe, which includes privacy and security directive. The CEN created this standard in 2008, which was then modified in 2010 with ISO approval. This standard's primary goal was to offer universal guidelines for creating interoperable electronic health systems. Efficiency, cost savings, and risk avoidance are the practical justifications for implementing standards.

Data Protection Act Kenya

The Data Protection Act (DPA) is essential for safeguarding medical records by ensuring the right handling of personal data. The primary focal points highlighted by DPA on the consequences for medical records are: The basic principles of the Data Protection Act (DPA) are as follows: Principles of legality, equity, and openness: Medical data must be processed in accordance with the law, in a just and open manner.

Purpose Restriction: Data should be gathered for specific, clear, and lawful intentions and should not be used in a way that is inconsistent with those intentions.

Data minimization refers to the practice of reducing the amount of data collected and stored to only what is necessary for a specific purpose or task. Collect and process only the data that is essential for the intended purposes.

Precision: Medical data must be precise and, when required, regularly updated.

Capacity Restriction: Personal data should be retained in a format that allows for the identification of persons only for as long as it is required for the intended purposes of processing the personal data.

Integrity and confidentiality: Data must be processed in a manner that guarantees adequate security, which includes safeguarding against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage.

Responsibility: Data controllers, such as healthcare providers, are required to show evidence of their adherence to these principles.

Details pertaining to medical records

Approval: Processing sensitive personal data, such as medical information, usually necessitates explicit agreement. Nevertheless, there are exemptions that apply to specific circumstances, such as instances involving public health concerns or cases where processing is indispensable for medical purposes.

Access rights: Patients own the entitlement to retrieve their medical records and acquire a duplicate of the information-maintained pertaining to them.

Rectification Right: Patients have the ability to request amendments to their medical records in the event that they discover any mistakes.

Right to Erasure: In specific situations, individuals have the right to seek the removal of their medical records, although this is contingent upon several caveats, particularly within hospital settings.

Data portability: Patients possess the entitlement to acquire and utilize their personal data for their individual objectives across various providers.

Security Protocols: Healthcare providers are required to establish and enforce suitable technical and organizational measures to safeguard medical records against unauthorized access, loss, or damage. This encompasses security measures like as encryption, access limits, and periodic audits.

Repercussions for Healthcare Providers

Educational and consciousness-raising activities: Personnel responsible for managing medical records must get training on the principles and practices of data protection.

Guidelines and protocols: It is essential to establish explicit rules and processes for the management of patient data, which should include specific methods for handling data breaches.

Data Protection Officers: Numerous healthcare institutions are obligated to designate a Data Protection Officer (DPO) to supervise adherence to data protection legislation. **Evaluations of the effects or consequences**: Performing Data Protection Impact Assessments (DPIAs) for initiatives that involve the handling of personal data to identify and reduce any hazards.

2.5.6 Common Data Security Architecture

This is an open and extensible software framework and API specification that usually addresses communication and data security requirements. It was originally developed by Intel Architecture Lab (IAL). The main objectives of Common Data Security Architecture were:

i. Encourage interoperable, horizontal standards

ii. Offer essential components of security capability to the industry.

The Common Data Security Architecture has three layers which include

System security services-this offers language interface adapter.

Common security services manager-this is a cryptographic service provider, which performs bulk encrypting, digesting and digital signature in addition there is trust policy modules which implement policies defined by authorities and level of trust required to perform certain actions. Security add-in modules- this layer provides modules that offer basic components in cryptographic algorithms and storage.

1. Categorization of Data

Data classification is the process of systematically organizing information based on its level of sensitivity and importance. This process helps organizations categorize their data so they can apply appropriate security measures according to the risk each type of data poses if compromised.

The objective of data classification is to ensure that sensitive information is adequately protected by implementing the right controls and precautions, reducing the risk of data breaches and ensuring compliance with relevant regulations. Common classifications include:

i. **Public**: Information that is safe for open disclosure and has no negative impact if shared widely.

ii. **Internal**: Data meant for use within the organization but not considered highly sensitive.

iii. **Confidential**: Sensitive information that should be restricted to authorized personnel to prevent harm to the organization.

iv. **Restricted**: The most sensitive data, where unauthorized access could cause significant damage, requiring the highest level of security.

2. Encryption of Data is the process of transforming information into an unreadable format using specialized algorithms, ensuring that only authorized parties can access it. The primary objective of encryption is to safeguard sensitive data, whether it's being transmitted across networks or stored on devices, from unauthorized access or breaches.

There are two common types of encryption techniques: **symmetric encryption**, such as the widely used Advanced Encryption Standard (AES), and **asymmetric encryption**, like RSA. Symmetric encryption uses the same key for both encryption and decryption, making it fast and efficient, particularly for large volumes of data. In contrast, asymmetric encryption employs a pair of keys—one public and one private—allowing for secure communication without needing to share the decryption key, although it is generally slower than symmetric methods. Both types of encryption are essential tools in maintaining the confidentiality and security of data in today's digital landscape.

3. Authorization Access control mechanisms are systems designed to enforce data restrictions based on predefined policies, ensuring that only authorized individuals or systems can access or modify sensitive information. The objective of these mechanisms is to protect data by regulating who can

view, edit, or interact with it, preventing unauthorized access and ensuring security across various environments.

There are several key techniques used for implementing access control:

i. **Role-Based Access Control (RBAC)**: Assigns permissions based on the roles users hold within an organization, ensuring that access is granted only according to their job functions.
ii. **Attribute-Based Access Control (ABAC)**: Uses attributes (such as user characteristics, resource types, or environmental conditions) to define access rules, providing a more flexible and context-aware approach.
iii. **Mandatory Access Control (MAC)**: A stricter model where access rights are determined by central authority policies, with users unable to modify or override permissions.

4. IAM (Identity and Access Management) Definition: Frameworks and technologies used to oversee and control digital identities and their authorization to access data.

Objective: Enables the process of secure authentication and authorization.

The components of the system include Single Sign-On (SSO), Multi-Factor Authentication (MFA), and identity governance.

Data masking is the process of obscuring or encrypting sensitive data to protect it from unauthorized access or disclosure.

Definition: The act of concealing specific information within a database in order to hinder illegal access.

Objective: Safeguards confidential data while allowing its utilization in non-operational settings.

Data Loss Prevention (DLP) is a system designed to prevent the loss or unauthorized disclosure of sensitive data.

Definition: Cybersecurity refers to the technologies and procedures implemented to identify and thwart unlawful access, utilization, or transmission of confidential information.

Objective: Safeguards data from unauthorized disclosure or security breaches.

The components are Network Data Loss Prevention (DLP), Endpoint Data Loss Prevention (DLP), and Email Data Loss Prevention (DLP).

7. Evaluation and Surveillance

Definition: The continuous monitoring and recording of data access and utilization.

Objective: Facilitates the identification and prompt handling of security breaches and ensures adherence to regulations.

Tools: Security Information and Event Management (SIEM) systems.

8. Data backup and restoration

Data backup refers to the processes and technology used to duplicate and store data in order to safeguard it against potential data loss.

Purpose: Ensures the ability to recover data in the event of unintentional removal, damage, or catastrophe.

Techniques: Complete backups, incremental backups, and differential backups.

Data governance refers to the overall management and control of an organization's data assets. It involves establishing policies, procedures, and guidelines to ensure the quality, integrity, and security of data throughout its lifecycle. Data governance refers to the set of policies, processes, and standards that are implemented to effectively manage and safeguard data.

Objective: Ensures the integrity, confidentiality, and availability of data while adhering to regulatory requirements.

The elements include data stewardship, data quality management, and compliance management.

10. Cybersecurity: Data encryption is the process of safeguarding data while it is being transmitted via networks. The objective is to mitigates unauthorized access and cyber assaults and technologies employed are firewalls, Intrusion Detection Systems (IDS), and Virtual Private Networks (VPNs).

11. Security measures implemented at the endpoints of a network to protect against unauthorized access and potential threats. Data protection on end-user devices refers to the safeguarding of information stored on these devices. Provides protection for devices such as computers, mobile

phones, and tablets from potential risks. Possible solutions include anti-malware software, endpoint detection and response (EDR) systems, and mobile device management (MDM) tools.

2.5.7 Summary of literature review

i. SecourHealth Framework (Simplicio et al., 2015)

Summary:

The SecourHealth framework addresses secure data communication in mobile health applications by proposing an architecture that ensures privacy, integrity, and authenticity of data exchanges. It focuses on the transmission of patient information in emergency situations and supports secure access to health data in real-time by authorized personnel.

Research Gaps:

Lack of extensive real-world testing and implementation in diverse healthcare environments, Limited evaluation of the framework's performance under varying network conditions, especially in low-resource settings and further study needed on user acceptance and integration into existing healthcare systems.

ii. Secure Mobile Data Collection System Framework (Gejibo, 2015)

Summary:

This framework presents a secure mobile system for data collection, designed to ensure confidentiality, integrity, and authenticity during data transmission between mobile devices and central servers. It leverages cryptographic techniques to protect sensitive data during collection, particularly in the healthcare and research sectors.

Research Gaps:

Insufficient consideration of scalability and performance in large-scale deployments, Limited focus on usability and user experience during mobile data collection and more comprehensive assessment of the framework's adaptability across different mobile platforms and environments.

iii. Enhanced Mobile Health Applications Cloud Computing Framework (Nkosi & Mekuria, 2010)

Summary:

This framework integrates mobile health applications with cloud computing, emphasizing scalability and improved data access through cloud storage and processing. The approach offers enhanced resource management, data sharing, and computation power for mobile health solutions.

Research Gaps:

Limited exploration of security and privacy concerns specific to cloud integration in healthcare, need for further examination of latency and real-time performance in resource-constrained environments

and Gaps in understanding the framework's compliance with healthcare regulations across different regions.

iv. Secure Mobile Banking Approach Framework (Elkhodr, 2012)

Summary:

Elkhodr's framework focuses on securing mobile banking transactions by proposing mechanisms for authentication, encryption, and data integrity. The framework aims to ensure that sensitive financial data is protected during transmission and storage in mobile banking systems.

Research Gaps:

Insufficient attention to evolving threats, such as malware and phishing in mobile banking, Limited research on user education and awareness regarding mobile banking security practices and lack of integration with emerging technologies like blockchain for enhancing transaction security.

v. Mobile Application Security System Framework (Floyd, 2006)

Summary:

This framework introduces strategies for securing mobile applications by addressing common vulnerabilities in mobile software. It covers security protocols, encryption techniques, and secure coding practices to mitigate risks associated with mobile apps.

Research Gaps:

Dated research, with limited consideration of newer threats, such as mobile malware, zero-day exploits, and advanced persistent threats, lack of focus on securing mobile applications in the cloud era, where apps are increasingly reliant on remote services and Gaps in addressing the specific challenges posed by modern mobile operating systems (e.g., Android and iOS).

vi. M-Health Decision-Making Framework for Community-Based Services (Maranda, 2016)

Summary:

Maranda's framework supports decision-making processes in community-based health services using mobile health (m-health) technologies. It emphasizes patient-centered care and collaborative decision-making among healthcare providers using mobile devices.

Research Gaps:

Limited analysis of the cultural and socio-economic factors affecting the adoption of m-health in community-based services, gaps in evaluating the effectiveness of the framework in diverse healthcare settings, particularly in rural and underserved communities and lack of detailed study on the interoperability of this framework with existing healthcare information systems.

vii. Framework for Assessing M-Health Challenges in South Africa (Leon et al., 2012)

Summary:

This framework outlines the key challenges facing the implementation of m-health systems in South Africa. It addresses issues related to infrastructure, regulatory policies, data security, and healthcare workforce readiness for m-health adoption.

Research Gaps:

Further exploration needed on sustainable models for m-health implementation in resource-limited settings, Lack of a comprehensive strategy to address the digital divide, particularly in rural areas and Gaps in understanding the role of government policies and private-sector partnerships in overcoming m-health challenges.

CHAPTER THREE

3. RESEARCH METHODOLOGY

3.1 Introduction

The chapter detailed the methodology employed in the study, with a particular focus on the significance of an electronic health system integration framework for secure M-health services, using the University of Nairobi Hospital as a case study. The study adopted a case study design, which involved collecting both qualitative and quantitative data from various respondents. Data was gathered through interviews with participants and by administering questionnaires to the target audience.

The chapter outlined several key aspects of the research process, including the research design, the population of the study, and the sample size. It also described the data collection methods used to

gather information from study participants and provided an overview of the tools and techniques employed for data analysis. This comprehensive approach ensured that the study was grounded in a robust methodological framework, enabling a thorough exploration of the research objectives.

3.2 Study Design

According to Wausi et al. (2009), a research design is a systematic plan that outlines the logical steps connecting research questions with the procedures for data collection, analysis, and interpretation, ensuring coherence throughout the study. Tarus et al. (2015) further emphasizes that in a descriptive study, the researcher can use the results obtained from a sample to generalize findings to the broader population.

In line with these perspectives, this study adopted a case study design. Both qualitative and quantitative data were collected from various respondents through a combination of interviews and questionnaires administered to the intended audience. This approach allowed for a comprehensive exploration of the research questions, enabling the study to derive meaningful insights and conclusions.

3.3 Study Population and sample size determination.

A systematic random sampling technique was employed in this study, ensuring that everyone had an equal opportunity to participate. The study population consisted of staff who use the University Health systems and the system developers at the University of Nairobi Hospital. A sample size of 44 system users and ICT personnel was selected. The researcher chose to include ICT staff because their

familiarity with the system's operations provided them with the necessary expertise on the University Health systems.

The study's three objectives were instrumental in formulating the research questions. The University of Nairobi Hospital was chosen as the study site because it has had an E-Health system in place for the past ten years, providing a robust context for collecting the required data.

Of the employees listed on the University of Nairobi Health Services website, forty-four (44) met the criteria for inclusion in the study. The sample size of the staff willing to participate was determined using Yamane Taro's sample size calculation formula (Yamane, 1967), ensuring that the sample was representative of the population.

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

Where:

n is the sample size of target population required for the study

N is the total population size of target population

e is the level of precision (error estimate) which is 0.05

$n = \frac{N}{1+N(e)2}$= $n = \frac{100}{1+100(0.05)2}$= 44 participants

44 people were therefore contacted to participate in the study.

Table 1: Sample Population Table for eHealth Framework Study (n=44)

Characteristic	**category**	**Number of participants**	**Percentage**
Gender	Male	24	54.5
	Female	20	45.5
Age Group	18-25	14	31.8
	26-35	16	36.4
	36-45	9	20.5
	46+	5	11.4
Education	Secondary	8	18.2
	Diploma	15	34.1
	Degree	16	36.4
	Masters	5	11.4

Role	Student	18	40.9
	Faculty	7	15.9
	Staff	11	25.0
	Patients	8	18.2
E-Health experience	None	12	27.3
	Beginner	18	40.9
	Intermediate	10	22.7
	Advanced	4	9.1

i. Gender: The sample has a slight majority of males (54.5%) compared to females (45.5%).

ii. Age Group: The largest age group is 26-35 years (36.4%), followed by 18-25 years (31.8%). This distribution reflects a younger adult population, which is common in university settings.

iii. Education: Most participants have either a bachelor's degree (36.4%) or a Diploma (34.1%), which is typical for a university environment.

iv. Role: Students make up the largest group (40.9%), followed by staff (25.0%), which is expected in a university setting.

v. eHealth Experience: The majority are beginners (40.9%) or have no experience (27.3%), which could be useful for studying the introduction of an eHealth framework.

3.4 Pre-test

To ensure that all study parameters were effectively assessed within the target group, the researcher conducted a pre-test of the developed questionnaire. This pre-testing involved distributing the questionnaire to a small, random sample of participants at the University of Nairobi Hospital. The purpose of this pre-test was to identify any potential issues or ambiguities in the questions. If any concerns or queries arose during the pre-test, the researcher made the necessary adjustments to the questionnaire. This process ensured that the tool was refined and capable of capturing the required information accurately during the actual study.

3.5 Testing for validity and reliability

The researcher had different experts verify the instruments by rating their performance and determining whether the instruments were consistent. A pilot study was carried out to ensure accuracy and consistency of the instruments.

3.6 Data Collection

The primary method of data collection for this project was through questionnaires. The questionnaires were left and picked later at an arranged time by the respondents. To ensure a high response rate and to help when respondents sought clarifications, there was follow-up via email, phone calls, and visits as needed. The questionnaires were administered to ICT staff and users who have roles in the

University Health System (UHS). In addition to questionnaires the researcher used observation and structured interviews to gain more information on the Security of University Health System.

3.7 Data Management

Once data was collected, the questionnaires were checked by the researcher to ensure that none was incomplete. Once this was done, the researcher stored these questionnaires in a lockable drawer where they were safe. Data entry was then done followed by data analysis and finally the researcher once again stored the questionnaires in a lockable cabinet.

3.8 Data Analysis and Presentation

The information from the respondents' completed questionnaires was coded and entered a computer statistics tool. Data analysis and the presentation of the findings were done using SPSS version 23.0, a statistical package for the social sciences. Correlation and Regression data analysis techniques were used.

3.8.1 Correlation analysis technique:

In statistics, correlation means that there is a relationship between various events. In statistics, the term "correlation" refers to the relationship between various occurrences.

To conducting a reliable correlation study, detailed observations of two variables are required, which gives us a benefit in terms of acquiring results. To examine the level at which the variables under study were related, Karl Pearson's as a measure of coefficient of correlation was used. The Pearson product-moment correlation coefficient denoted as r was primarily used to gauge the level of association between two variables and ranges from +1 to -1. Lack of relationship between variables is denoted by zero value. Where there is a positive relationship, a figure greater than zero is indicated whereas a negative relationship is indicated by a figure less than zero.

Simple metrics: Findings from research can be categorized easily. The results can be between -1.00 and 1.00. There can only be three possible overall conclusions from the analysis.

3.8.2 Regression Analysis technique:

A multiple regression analysis was undertaken to further gauge the association among the independent variables on Security of M-health at the University of Nairobi Hospital. To aid this SPSS V 21.0 was used to facilitate the outcomes of the multiple regressions for the study. Predict research in the near and long term, Understand service security levels. Review and comprehend how various factors affect each of these things. The extent to which changes in the dependent variable (secure service) was influenced by all the four independent variables (Information integrity, Pseudonymization, information confidentiality and information availability) was explained by the coefficient of determination.

$$Yi = f(xi, \beta) + \Theta i$$

Where Y was the dependent variable which was secure M-health system

Xi was the independent variable of Confidentiality.

Xii was the independent variable of pseudonymization.

Xiii independent variable integrity

Xiv independent variable availability

Thus

$$Y = (Xi + Xii + Xiii + Xiv, \beta) + \epsilon i$$

In both techniques, results were presented using tables, frequency charts and graphs, and the findings were presented using tables, graphs, bar charts, pie charts, mean and standard deviation.

3.8.3 Ethical Considerations

Prior to the commencement of the study, approval to conduct research was obtained from the Mount Kenya University (MKU) Ethical Review Committee. Additionally, a clearance certificate from the National Commission for Science, Technology and Innovation (NACOSTI) was secured. These approvals were essential to ensure that the research adhered to ethical standards and regulations, thereby safeguarding the integrity of the study and the rights of the participants involved.

CHAPTER FOUR

4. RESEARCH FINDINGS AND DISCUSSIONS

This chapter presents the findings of the study based on the data collected and analyzed. The purpose of this chapter is to provide a detailed account of the results obtained, highlighting key patterns, relationships, and trends that emerged from the data. The findings were organized in accordance with the research questions outlined in Chapter One and were presented in a clear and systematic manner to facilitate understanding.

The results were discussed with reference to the theoretical framework and literature review provided in earlier chapters, offering insights into how the data supports existing knowledge in the field. Where

applicable, tables, graphs, and charts were used to visually represent the data, ensuring that complex information is conveyed in an accessible and meaningful way.

The chapter is divided into several sections, each corresponding to a specific research question or theme. Each section begins with a brief overview of the research question it addresses, followed by a presentation of the relevant findings. The chapter concludes with a summary of the key results, which will be further discussed in Chapter Five, where the implications of these findings are explored in greater detail.

4.1 Results

The main objective of this study sought to design a model for electronic health system Integration framework for secure M-Health information systems.

This objective was achieved and managed to evaluate and investigate the existing frameworks for electronic health Integration. The review of the current form of framework revealed that mobile based Health Information systems are unreliable and do not enable professional health workers access to patients' data at any given time.

The results from this project revealed that over 70% believed introduction of Confidentiality, Integrity and availability on the security of M-health systems would make University Health systems processes convenient.

The second objective was to develop a framework for secure integration of M-health systems.

The framework was developed, built and tested. University Health System framework was found to be working well, consisting of entities for security measures.

The third and final objective was to validate the proposed framework. Evaluation of its applicability and usability revealed that it can reduce the vulnerability and improves security level of university health Systems, thus making seamless intervention where M-Health security concern is raised.

The significance of a comprehensive information security of M-health systems at the University of Nairobi Hospital, objective 1 results.

The first question is to find out the period for which the respondents have worked in the hospital.

Table 2:Period which respondents have worked in the Hospital.

Choice	Frequency	Percentage	Cumulative percentage
Over 20 years	3	6.82	6.82
10 to 20 years	4	9.10	15.92
5 to 10 years	20	45.46	61.38
Less than 5years	17	38.62	100.00
Total	44	100.00	

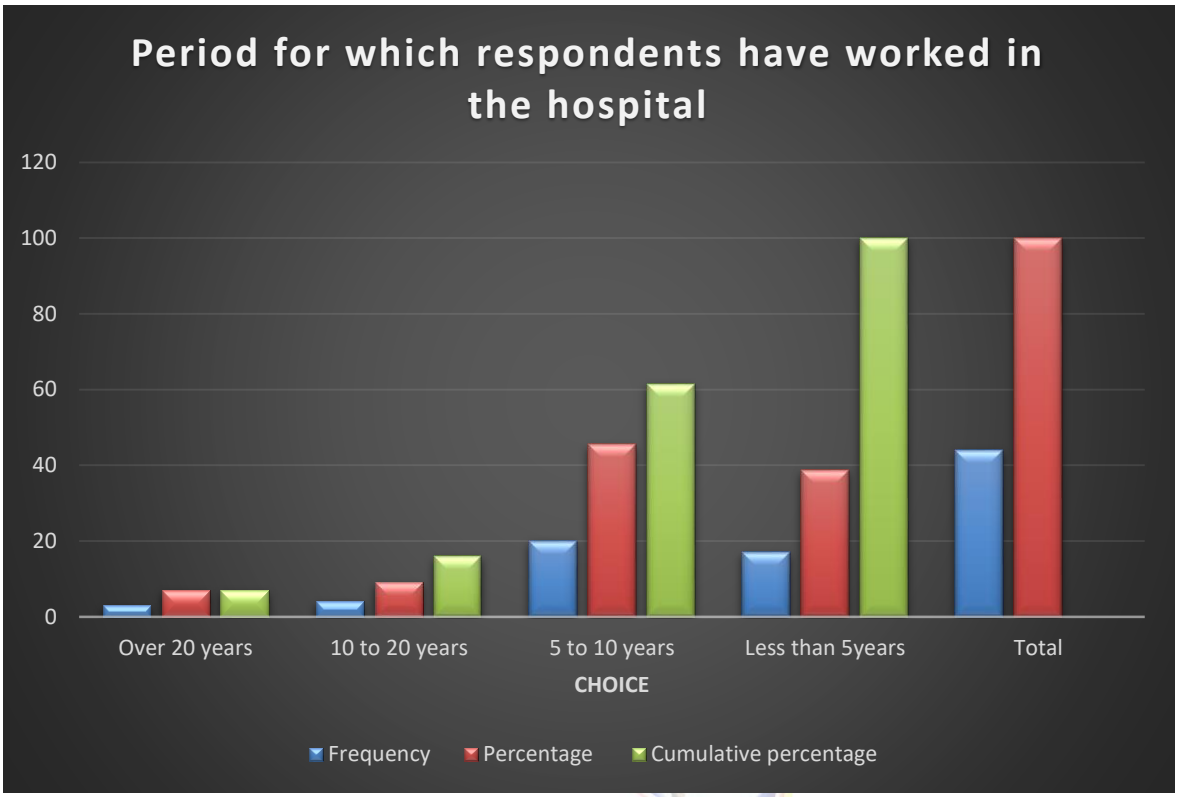


Figure 14: Period for which respondents have worked in the hospital.

Based on 44 respondents, 6.82% of them indicated to have worked in hospital for over 20years. 9.10 % had worked for between 10 to 20 years. Another 45.45% had worked in hospital between 5 to 10 years and the last 38.62% had worked in hospital a period less than 5 years.

From the results the researcher noted a good number of staff had relative experience at the hospital over 5years.

The second question was to find out the academic qualification for the respondents.

Table 3: Academic qualification for the respondents

Choice	Frequency	Percentage	Cumulative percentage

Graduate	21	47.73	47.73
Undergraduate	12	27.27	75.00
Diploma	11	25.00	100.00
Other	0	0	100.00
Total	**44**	**100**	**100**

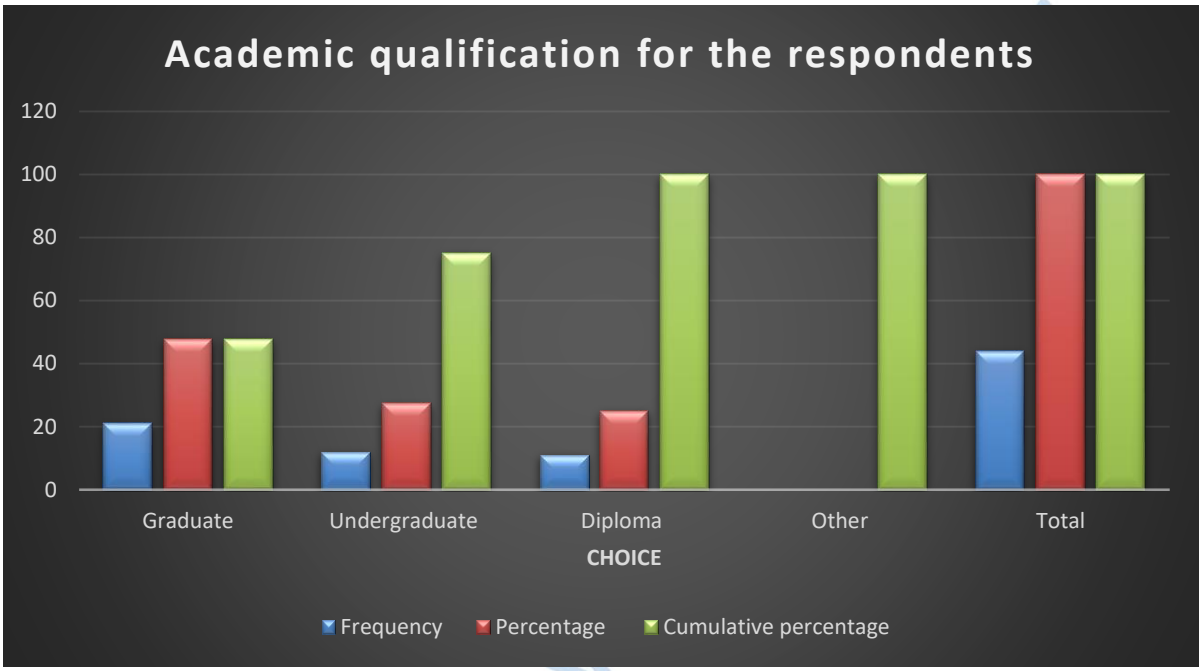


Figure 15: Academic qualification for the respondents

Out of 44 respondents, 47.73% of respondents hold Graduate. 27.27% holds Undergraduate and lastly 25.00% diploma holders.

From the table above, evidently, the vast majority of respondents' i.e., 75.00%, have undertaken education with research component in it and understand the research activities well.

The questions intend was to know the level of Hospital ensuring that all actors add the medical records as soon they are through with the patient to ensure completeness and reliability.

Table 4: Timely addition of medical records in ensuring completeness.

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	14	31.80	31.80
Agree	15	34.10	65.90
Neutral	15	34.10	100.00
total	**44**	**100.00**	**100**

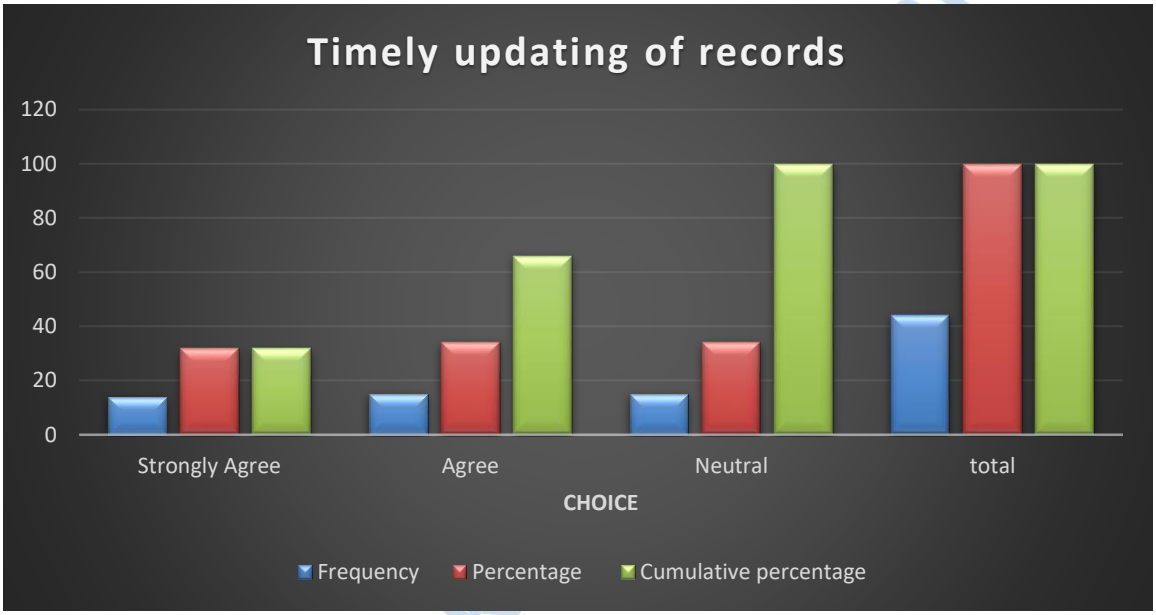


Figure 16:Timely updating of records

From a total of 44 responses, 31.80% of the respondents strongly agreed that timely addition of medical records in ensuring completeness is observed, 34.10% agreed. A similar 34.10% were neutral.

This indicates that if Electronic Health System Integration Framework for Secure M-Health Service, 65.90% of staff would find it helpful.

Researcher asked respondents if the hospital has ensured accuracy of medical records though protection of information against loss.

Table 5: Response on accuracy of medical records through protection of information against loss.

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	6	13.64	13.64
Agree	24	54.54	68.18
Neutral	14	31.82	100.00
Total	35	100.00	100

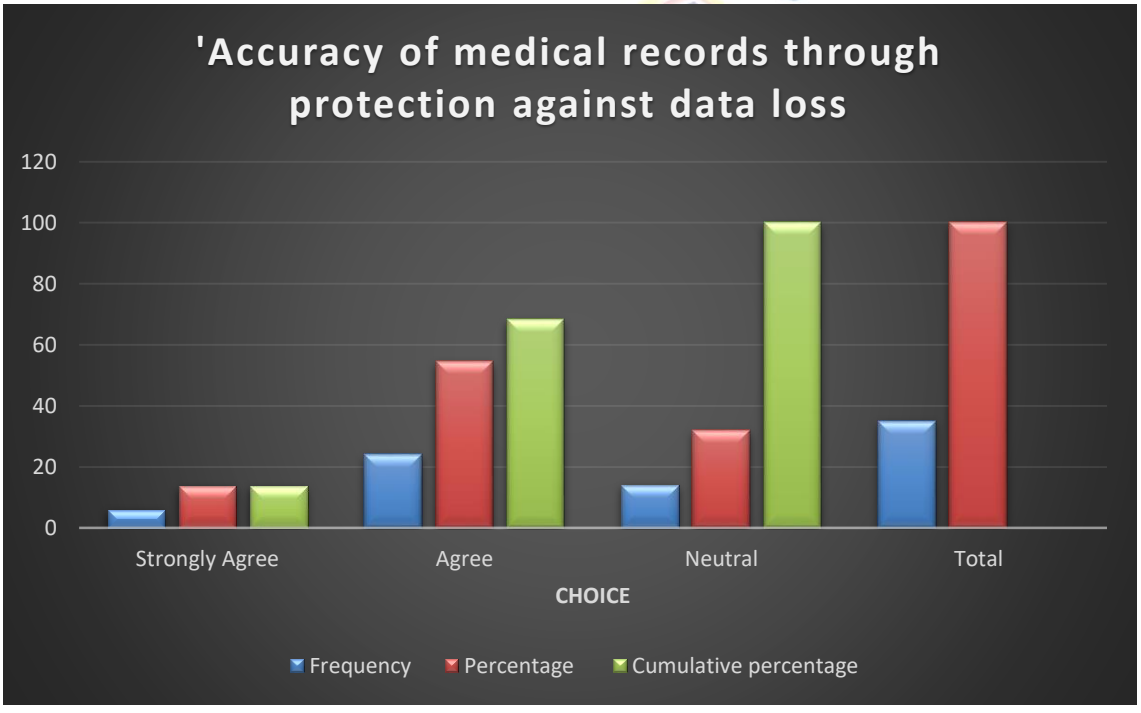


Figure 17:Accuracy of medical records through protection against data loss

Out of 44 responses, 13.64% of the respondents strongly agreed on accuracy of medical records through protection of information against loss. Another 54.54% agreed on the same. 31.82% of the respondents were neutral. So, we can conclude that protection of information against loss of medical records was key.

The researcher asked the respondents whether the hospital ensured that medical records were protected against distortion while in transmission through electronic media.

Table 6: Security on medical records while in transmission.

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	11	25.00	25.00
Agree	20	45.45	70.45
Neutral	13	29.55	100.00

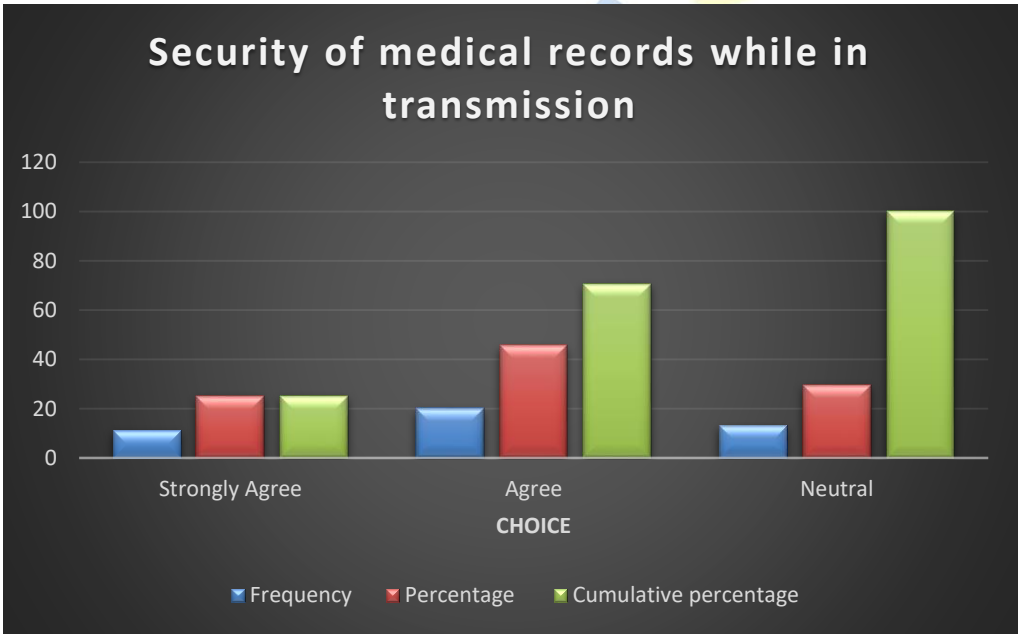


Figure 18: Security of medical records while in transmission.

To the above question, 44 responded. Out of which 25.00% strongly agreed presence of security on medical records while on transmission. 45.45% agreed too. 25.81%, while 29.55% are neutral. This means that 70.45% respondents believed in the availability of secure environment in medical records transmission.

The researcher asked respondents for thought about the Hospital in ensuring that employees have basic IT knowledge to key in accurate data.

Table 7:Responses on whether the Hospital ensured its employees have basic IT knowledge to key in accurate data.

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	10	22.72	22.72
Agree	19	43.20	65.92
Strongly Disagree	7	15.90	81.82
Neutral	8	18.18	100.00
Total	44	100.00	100.00

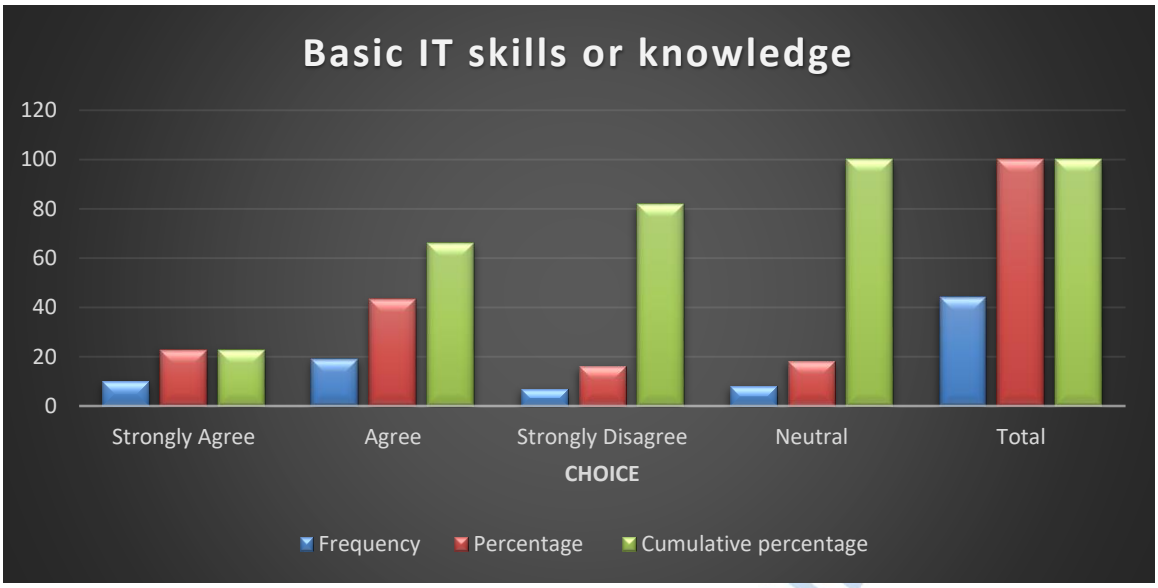


Figure 19:Basic IT Skills or knowledge

There were 44 responses, 22.372 strongly agreed. 43.20% Agreed, 15.90% Strongly Disagreed, while 18.18% were neutral. Guided by the responses, the researcher came to the conclusion that most of respondents were satisfied that the hospital ensured employees have basic IT knowledge thus using the proposed system was viable.

The researcher asked respondents whether Passwords have been put in computers for protection of data.

Table 8: Protection of data through computer passwords

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	13	29.55	29.55
Agree	23	52.27	81.82
Neutral	8	18.18	100.00

Total	44	100.00	100

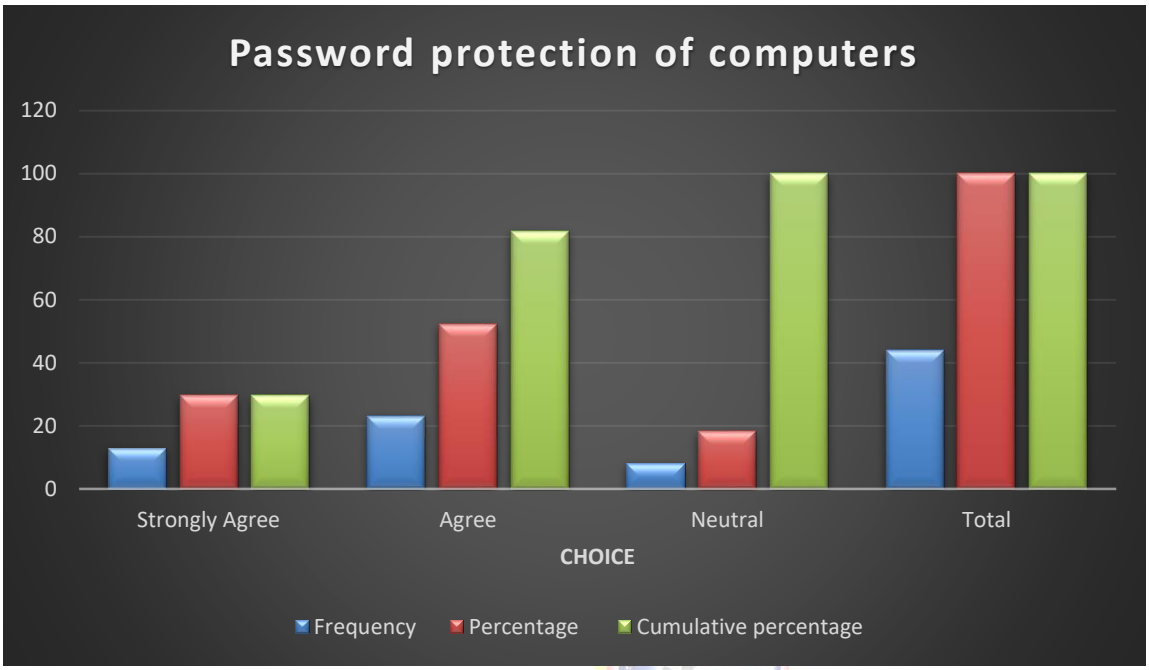


Figure 20:Password protection of computers.

Most respondents strongly agreed or agreed with protection that has been put in place.

The researcher asked respondents whether The Hospital has ensured that the system has various users with different roles to avoid unauthorized access of patients' data.

Table 9: Protection of data through roles and rights of access to patients' data

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	8	18.18	18.18
Agree	17	38.64	56.82
Neutral	19	43.18	100.00
Total	44	100.00	100

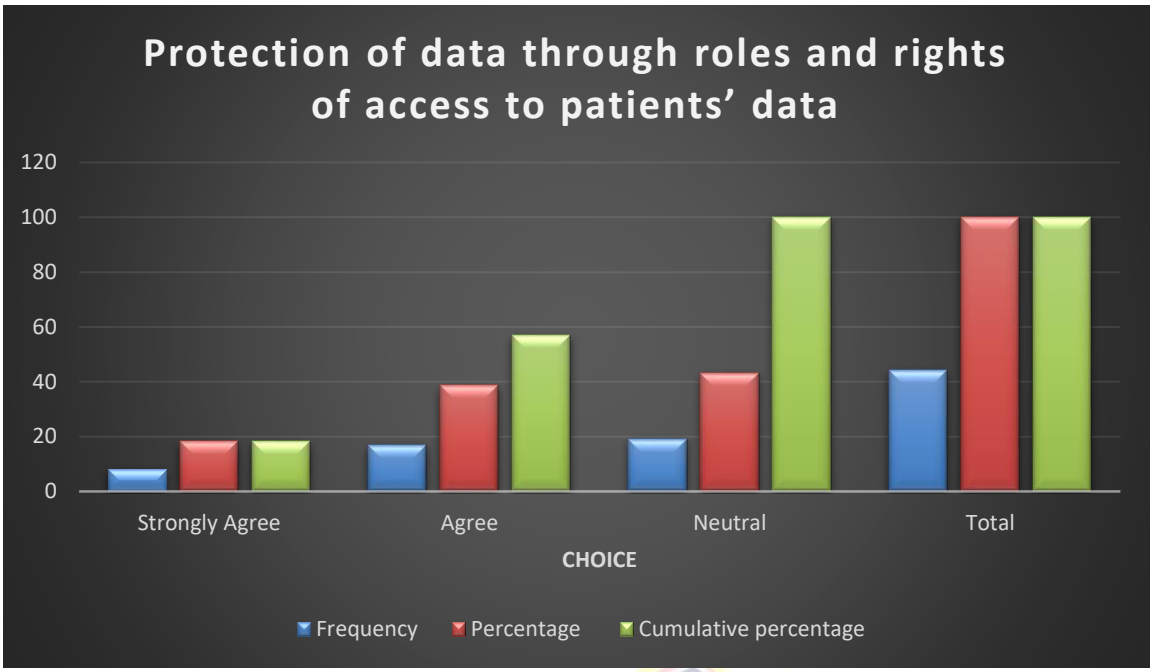


Figure 21:Protection of data through roles and rights of access to patients data.

The researcher asked respondents if The University Health system is always up and running

Table 10:Availability of system

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	7	15.91	15.91
Agree	14	31.82	47.73
Disagree	10	22.72	70.45
Neutral	13	29.55	100.00
Total	44	100.00	100.00

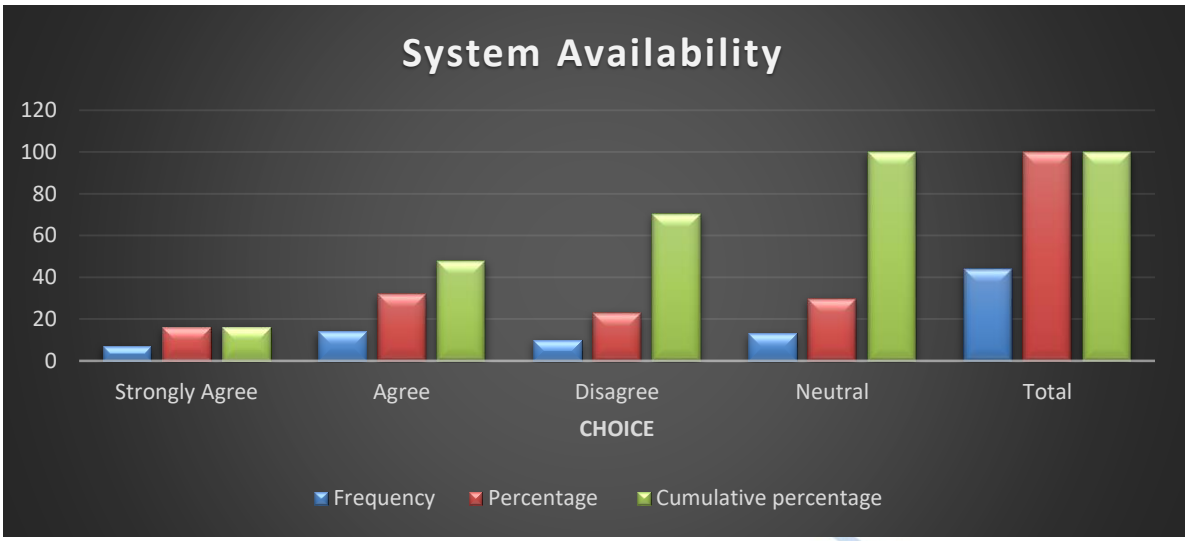


Figure 22: System availability.

Nearly a half of the respondents agreed that the system is always available.

The researcher asked respondents whether the flow of information in the University Health system is traceable through logging and documentation

Table 11: Traceability flow of information

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	12	27.27	27.27
Agree	13	29.55	56.82
Disagree	9	20.45	77.27
Neutral	10	22.73	100.00
Total	44	100.00	

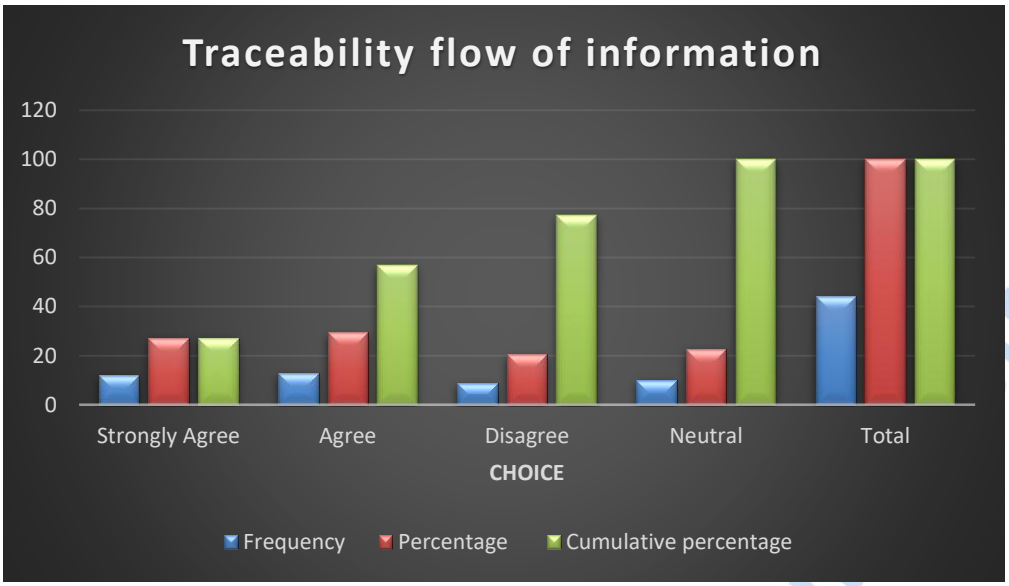


Figure 23:Traceability flow of information.

The researcher asked respondents if there is an offsite backup of the patient data.

Table 12: Offsite backup availability

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	6	13.64	13.64
Agree	17	38.64	52.28
Neutral	21	47.72	100.00
Total	44	100.00	100.00

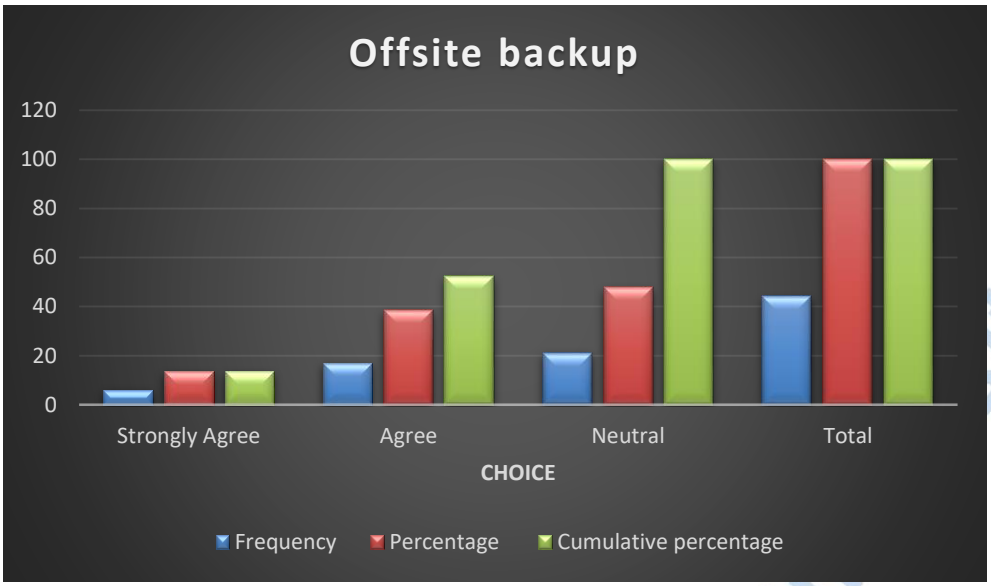


Figure 24:Offsite backup.

The researcher asked respondents if Healthcare professionals have access to patients' information when needed.

Table 13:Accessibility of information by medical professionals

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	9	20.45	20.45
Agree	25	56.82	77.27
Disagree	10	22.73	100.00
Total	44	100.00	100

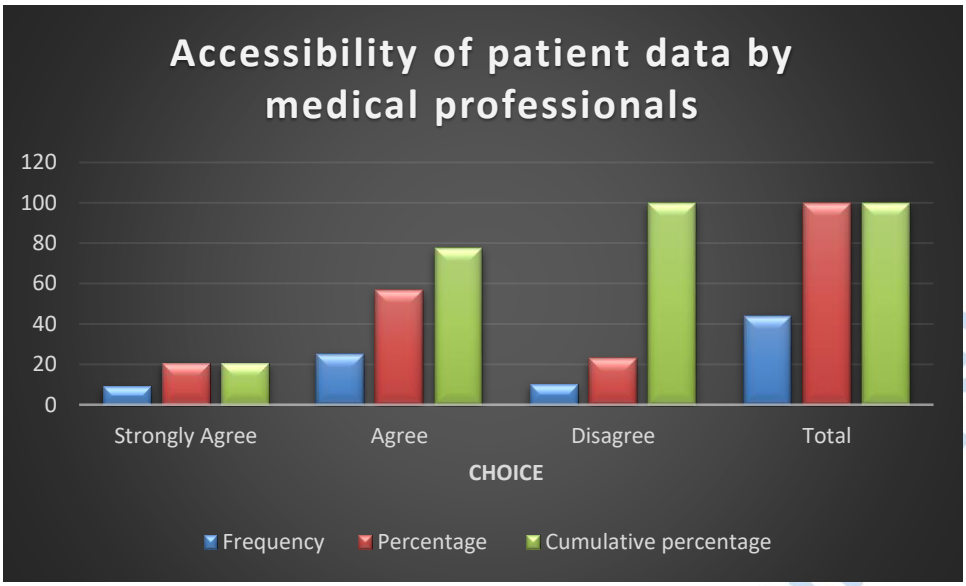


Figure 25: Accessibility of patient data by medical professionals

The researcher asked respondents if the computer being used has an updated Antivirus

Table 14: Use of Anti-Virus

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	5	11.36	11.36
Agree	20	45.45	56.81
Disagree	3	6.83	63.64
Neutral	16	36.36	100.00
Total	44	100.00	

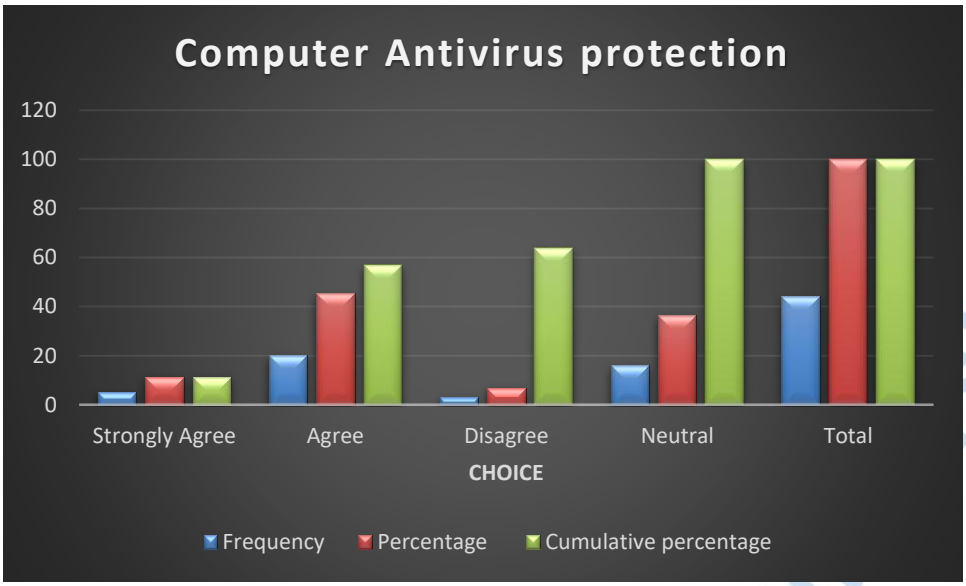


Figure 26:Computer Antivirus protection.

The researcher asked respondents if Patient records are always Pseudonymized.

Table 15:Patient records Pseudonymized.

Choice	Frequency	Percentage	Cumulative percentage
Strongly Agree	1	2.27	2.27
Agree	4	9.10	11.37
Disagree	4	9.10	20.47
Strongly Disagree	19	43.18	63.65
Neutral	16	36.35	100.00
Total	44	100.00	100

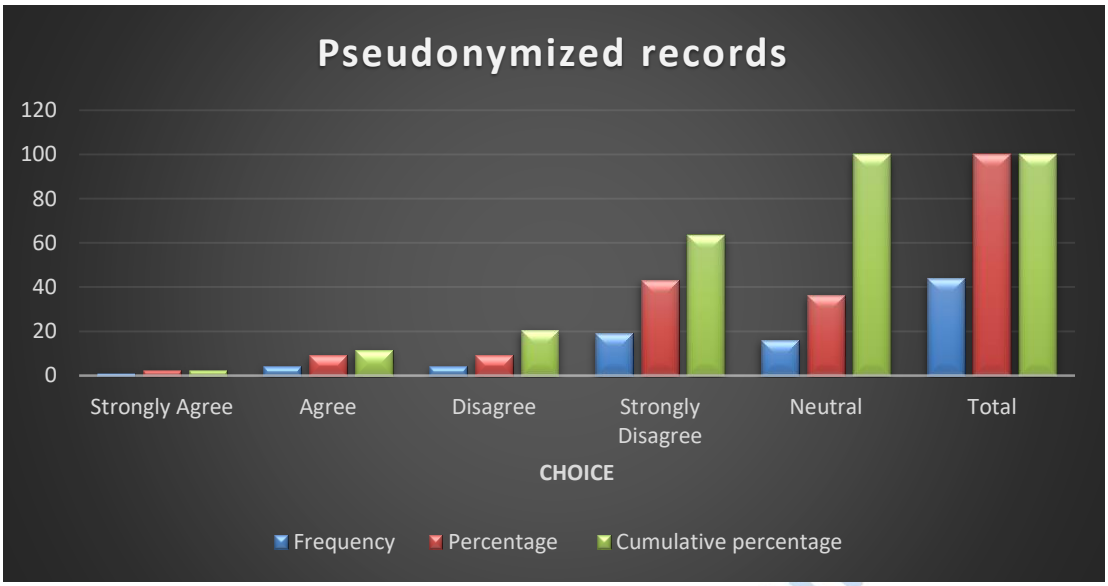


Figure 27:Pseudonymized records.

4.2 Relationship between independent variables on Security of M-Health Systems

4.2.1 Correlation Analysis

To examine the level at which the variables under study were related, Karl Pearson's as a measure of coefficient of correlation was used. The Pearson product-moment correlation coefficient denoted as r is primarily used to gauge the level of association between two variables and ranges from +1 to -1. Lack of relationship between variables is denoted by zero value. Where there is a positive relationship, a figure greater than zero is indicated whereas a negative relationship is indicated by a figure less than zero. The findings are as at

Table 16: Correlation Analysis

Variables	Confidentiality	Integrity	Availability	EMR Pseudonymization
Confidentiality	1	0.56	0.34	0.62
Integrity	0.56	1	0.48	0.45
Availability	0.34	0.48	1	0.29
EMR Pseudonymization	0.62	0.29	0.29	1

The high correlation (r = 0.62) suggests that systems with strong confidentiality measures also tend to implement pseudonymization effectively. This correlation indicates that protecting patient data aligns with anonymization efforts. A moderate positive correlation (r = 0.48) indicates that systems designed with data integrity in mind often enhance data availability, likely due to more reliable data handling practices. A weak correlation (r = 0.29) shows limited direct association, suggesting availability does not significantly affect pseudonymization efforts.

4.2.2 Regression Analysis

A multiple regression analysis was undertaken to further gauge the association among the independent variables on Security of M-health in University of Nairobi Hospital. To aid this, SPSS V 21.0 was used to facilitate the outcomes of the multiple regressions for the study.

The extent to which changes in the dependent variable (Security of M-health) is influenced by all the independent variables (Information integrity, information confidentiality, information availability and Pseudonymization of EMR) is explained by the coefficient of determination.

Table 17:Model Summary

Model	R	R Square	Adjusted Square	R Std. Error of the Estimate
1	.849[a]	0.72	0.70	0.0131

a. Predictors: (Constant), Information integrity, information confidentiality, information availability and EMR Pseudonymization.

b. Dependent Variable: Security of M-health

Table 16 shows **model summary** of regressed variable of the study. The independents variables in the study explain 72% effect of level of information security as applied by the University of Nairobi hospital and how it affects Security of M-health system as represented by R Squared (Coefficient of determinant). This therefore means 28% are other factors not studied in this research that influence Security of M-health.

Table 18:Anova (Analysis of Variance)

$$F = between\ group \frac{variance}{} within\_group\ variance$$

Variable	F-Value	P-value	Interpretation
Confidentiality	7.58	**<0.01**	Significant effect
Integrity	6.33	**<0.01**	Significant effect
Availability	4.82	**0.01**	Significant effect
EMR pseudonymization	8.21	**<0.01**	Significant effect

The F-value of 7.58 ($p < 0.01$) suggests a significant difference in EMR security across the levels of confidentiality. This finding indicates that higher confidentiality is associated with stronger EMR

security, highlighting its importance as a protective measure. The F-value of 6.33 ($p < 0.01$) indicates a significant impact on EMR security across integrity levels. This result implies that data integrity improvements have a substantial effect on securing EMRs. With an F-value of 4.82 ($p = 0.01$), availability also has a significant effect on EMR security, although to a lesser extent than confidentiality and pseudonymization. This suggests that systems designed to ensure reliable data access contribute to EMR security but may be less critical than confidentiality. The F-value of 8.21 ($p < 0.01$) is the highest among the variables, showing that pseudonymization levels have a significant effect on EMR security. This finding indicates that effective pseudonymization practices play a crucial role in enhancing EMR security, likely due to their focus on patient identity protection.

Table 19:Coefficient of Determination

Predictor	**Coefficient (β\betaβ)**	**Standard Error**	**t-value**	**p-value**
Intercept	0.82	0.18	4.56	< 0.01
Confidentiality	0.72	0.14	5.14	< 0.01
Integrity	0.45	0.13	3.46	< 0.01
Availability	0.33	0.11	3.00	< 0.01
EMR Pseudonymization	0.54	0.12	4.50	< 0.01

- **R-squared**: 0.72
- **Adjusted R-squared**: 0.70

The overall equation model for Security of M-health, Information integrity, information confidentiality, and information availability and EMR pseudonymization was as follows:

Security of EMR=β0+β1(Confidentiality)+β2(Integrity)+β3(Availability)+β4

(EMR Pseudonymization) +ϵ

where:

- β0\beta_0β0 is the intercept,
- β1,β2,β3,β4\beta_1, \beta_2, \beta_3, \beta_4β1,β2,β3,β4 are the coefficients for each predictor, and
- ϵ\epsilonϵ is the error term.

The coefficient for confidentiality (0.72) shows it is the most significant predictor of EMR security, with a strong positive relationship ($p < 0.01$). This suggests that higher confidentiality measures greatly enhance the security of EMR systems. Integrity has a positive and significant impact on EMR security, with a coefficient of 0.45 ($p < 0.01$). This indicates that improvements in data accuracy and consistency contribute substantially to the protection of EMRs. Availability's positive coefficient of 0.33 ($p < 0.01$) suggests that systems with better data availability are associated with enhanced security. This implies that reliable access contributes, albeit to a lesser extent, to the overall security framework. The coefficient for EMR pseudonymization (0.54) reflects a significant positive effect on EMR security ($p < 0.01$). This result highlights the importance of identity protection in achieving robust EMR security. The R-squared value of 0.72 indicates that 72% of the variance in EMR security can be explained by the independent variables, demonstrating a strong model fit.

4.3 Discussion of Findings

The correlation analysis highlights critical relationships among data security principles in EMR systems. Notably, the strong association between confidentiality and pseudonymization reinforces the importance of integrating both to enhance patient privacy. Moreover, while integrity and availability are moderately correlated, they do not strongly influence pseudonymization practices, indicating independent factors may govern these aspects.

The regression analysis reveals that confidentiality, integrity, availability, and EMR pseudonymization all positively impact the security of EMRs, with confidentiality showing the strongest predictive power. These findings suggest that healthcare organizations focusing on these core security principles can better protect EMRs, particularly by prioritizing confidentiality and pseudonymization.

The ANOVA results indicate significant differences in EMR security based on the levels of confidentiality, integrity, availability, and EMR pseudonymization, with pseudonymization having the strongest impact. These findings highlight the importance of a multifaceted approach to EMR security, suggesting that healthcare organizations should prioritize these four areas to enhance data protection comprehensively.

Like the study findings, Brundtland, (2001) noted that health care delivery has been noted as one of the services deliveries that require high involvement of the consumer in the

consumption process (Peprah, 2014). The customer is involved throughout the entire Security of M-health process. Information security breaches can result in clinical diagnoses that are incorrect, which can have serious consequences for patients.

4.4 Framework Design.

The framework design entailed requirement analysis, data management layer, security features required and the interoperability considerations. The Requirement Analysis phase serves as the foundation for any project, informing and shaping all subsequent components. This initial step involves understanding and documenting the needs and expectations of the system or application. It feeds directly into the design of the Data Management Layer, Security Features, and Interoperability Considerations, ensuring that all key aspects are aligned with user requirements.

4.4.1 Requirement Analysis

A detailed analysis of the security and interoperability requirements was essential to ensure the successful integration of mHealth services within the hospital's existing eHealth infrastructure. This analysis involved identifying the specific needs and challenges that the framework must address.

4.4.1.1 Security Requirements

a) **Data Confidentiality:** The framework ensured that sensitive patient data is protected from unauthorized access. This required robust encryption methods for data at rest and in transit.

b) **Data Integrity:** To prevent unauthorized alterations, the framework included mechanisms that guarantee the integrity of health data exchanged between mHealth applications and the eHealth system.

c) **User Authentication and Authorization:** The system implemented multi-factor authentication (MFA) to verify user identities. Role-based access control (RBAC) should be employed to ensure that only authorized personnel can access specific information or functionalities.

d) **Audit Trails:** The framework should maintain detailed logs of all access and changes to the system, supporting accountability and traceability.

e) **Pseudonymization**-The framework should entail substituting identifiable information with pseudonyms, so safeguarding people's privacy while enabling the utilization of data for analysis and research purposes.

4.4.1.2 Interoperability Requirements

a) **Standards Compliance:** The framework should adhere to established healthcare interoperability standards such as HL7 (Health Level Seven) and FHIR (Fast Healthcare Interoperability Resources). This ensures seamless communication between mHealth applications and existing hospital systems.

b) **Data Exchange:** The framework must support the smooth exchange of data between diverse mHealth applications and the hospital's electronic health record (EHR) system, ensuring real-time updates and data consistency.

c) **Scalability:** The framework should be scalable to accommodate an increasing number of users, devices, and mHealth applications without compromising performance or security.

4.4.2 Framework Architecture

The proposed framework was designed using a modular architecture that supports secure and interoperable integration of mHealth services with the hospital's existing eHealth system.

4.4.2.1 Modular Design

a) **Core Components:** The architecture was divided into core components, including a Security Module, an Interoperability Engine, and a Data Management Layer. Each component handled specific functions related to security, data exchange, and system integration.

b) **Security Module:** This module was responsible for implementing encryption, authentication, authorization, and audit trail management. It integrates with the hospital's existing security infrastructure and provides APIs for secure communication with mHealth applications.

c) **Interoperability Engine:** This engine facilitated the translation and routing of data between mHealth services and the hospital's EHR system. It supports HL7 and FHIR standards, ensuring compatibility with various data formats and protocols.

d) **Data Management Layer:** This layer handled the storage, retrieval, and processing of health data. It was designed to work with encrypted data and supports efficient querying and reporting. This has various components as discussed below:

i. **Data Storage:** This component is responsible for determining how and where data is stored in the system. It addresses the architecture of storage solutions, whether using traditional relational databases, NoSQL systems, or cloud storage options. The focus is on ensuring that data is stored efficiently, securely, and with the necessary redundancy for recovery and scalability.

ii. **Data Processing:** This handles the transformation and computation of data. Once data is stored, it often needs to be processed to extract valuable insights. This might involve cleaning, aggregating, or manipulating data, using ETL (Extract, Transform, Load) processes or real-time stream processing frameworks.

iii. **Data Retrieval:** Accessing and querying data is crucial for both end-users and systems. This component manages the mechanisms that allow users or applications to search, retrieve, and query stored data efficiently, ensuring minimal latency and maximal throughput.

4.4.2.2 Secure APIs

a) **API Gateway:** The framework included an API gateway that manages all incoming and outgoing API requests. The gateway enforced security policies, including rate limiting, input validation, and authentication checks.

b) **API Encryption:** All data transmitted via APIs is encrypted using TLS (Transport Layer Security). This protects data from being intercepted or tampered with during transmission.

4.4.2.3 Encryption Methods

a) **Data at Rest:** Patient data stored within the hospital's systems is encrypted using AES (Advanced Encryption Standard) with a 256-bit key. This ensured that even if the storage is compromised, the data remains inaccessible without the encryption key.

b) **Data in Transit:** Data exchanged between mHealth applications and the hospital's systems is protected using TLS. This encryption method ensures the confidentiality and integrity of data during transmission.

4.4.2.4 Data Integrity Mechanisms

a) **Digital Signatures:** Digital signatures are used to verify the authenticity and integrity of data sent between mHealth services and the hospital's eHealth system. Any alterations to the data after it has been signed are detected, preventing unauthorized modifications.

b) **Hashing:** Health records are hashed using secure algorithms (e.g., SHA-256) to create unique data fingerprints. These hashes are compared before and after transmission to ensure that no tampering has occurred.

4.4.3 Security Features

The security features of the framework are designed to provide comprehensive protection against unauthorized access, data breaches, and other security threats.

4.4.3.1 Multi-Factor Authentication (MFA)

a) **User Verification:** MFA requires users to provide two or more verification factors before gaining access to the system. These factors include something the user knows (password), something the user has (a smartphone for OTP), and something the user is (biometrics).

b) **Integration with Hospital Systems:** The MFA system was integrated with the hospital's existing user management systems, ensuring that it does not disrupt workflow while enhancing security.

4.4.3.2 Secure Communication Protocols

a) **Transport Layer Security (TLS):** TLS is employed to encrypt all data communications between mHealth applications and the hospital's systems. This protocol ensures that sensitive

information such as patient records and authentication credentials are protected against eavesdropping and man-in-the-middle attacks.

b) **Virtual Private Network (VPN):** A VPN is implemented for remote access to the hospital's systems, ensuring that all external communications are secure.

4.4.3.3 Access Control and Authorization

a) **Role-Based Access Control (RBAC):** The framework uses RBAC to manage permissions based on user roles within the hospital. For instance, doctors, nurses, and administrative staff have different levels of access to patient data.

b) **Access Logs and Monitoring:** All access to patient data and system functionalities is logged. These logs are regularly monitored for any unusual or unauthorized activity, providing an additional layer of security.

4.4.4 Interoperability Considerations

Interoperability is critical to the framework's success, allowing mHealth services to work seamlessly with the hospital's existing E-Health systems.

4.4.4.1 Adoption of HL7 and FHIR Standards

a) **Health Level Seven (HL7):** HL7 standards are adopted for the exchange, integration, sharing, and retrieval of electronic health information. The framework supports HL7 messaging formats, which are widely used in healthcare data exchange.

b) **Fast Healthcare Interoperability Resources (FHIR):** FHIR is implemented to enhance interoperability by providing a standardized way to represent and exchange healthcare information. FHIR is particularly useful for mobile health applications due to its flexibility and support for RESTful APIs.

4.4.4.2 Data Mapping and Transformation

a) **Data Translation:** The framework includes tools for mapping and transforming data from different mHealth applications to the standard formats used by the hospital's EHR system. This ensures that data from various sources can be accurately integrated and used within the hospital's systems.

b) **Consistency Checks:** The framework performs consistency checks during data exchange to ensure that all integrated data conforms to the required standards and formats, reducing the risk of errors or data loss.

4.4.4.3 Scalability and Extensibility

a) **Modular Architecture:** The framework's modular design allowed for easy addition of new mHealth services or updates to existing ones without disrupting the system's operation.

b) **Futureproofing:** The framework was designed to be adaptable to future changes in technology and healthcare standards, ensuring that it remains relevant and effective as new mHealth services and technologies emerge.

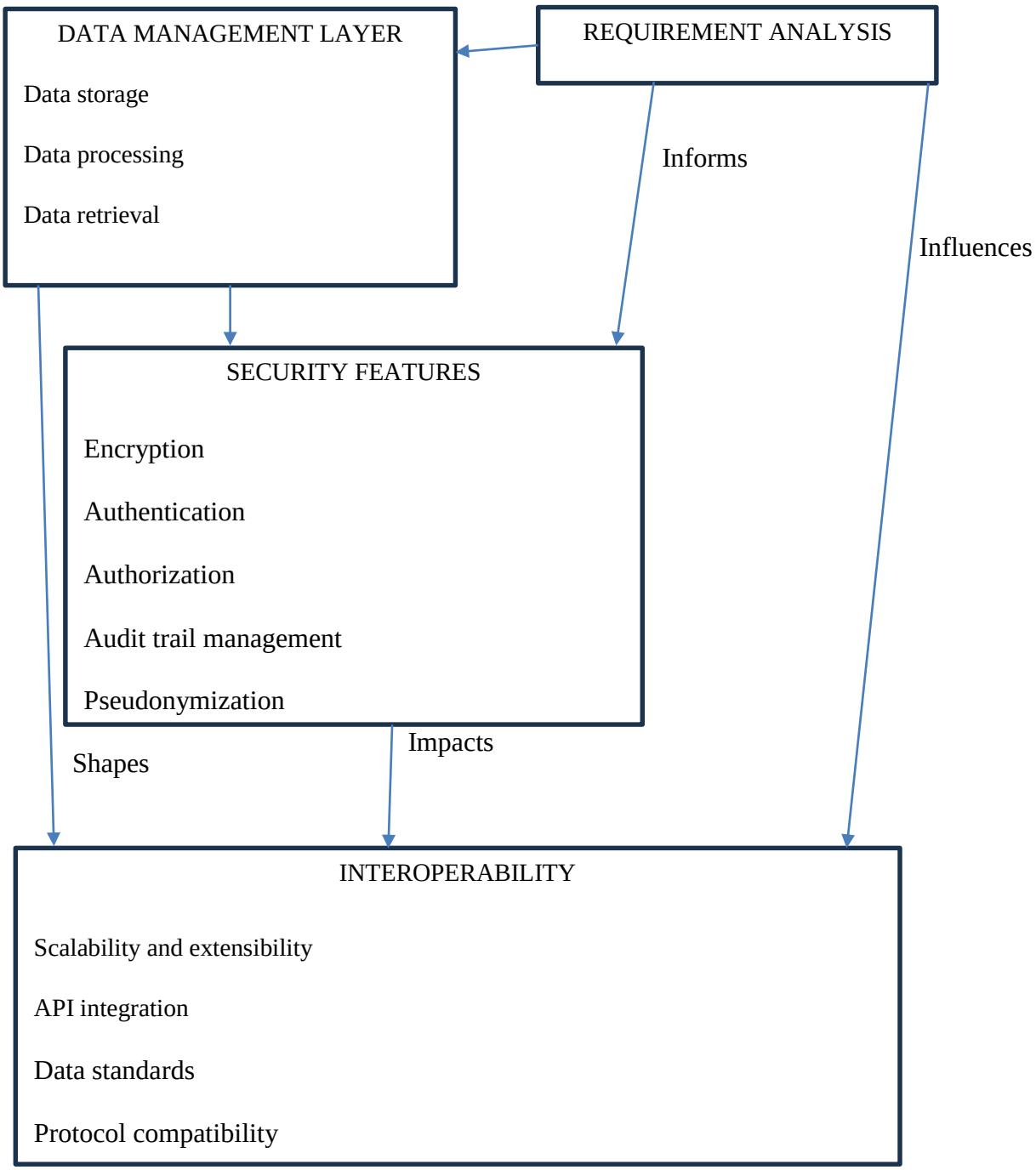


Figure 28:Proposed E-Health Security Framework (PEHSF)

1. Requirement Analysis: This is the starting point, where the security needs and constraints are identified in the system.

2. Data management layer: Based on the requirements, the overall structure of the security framework is designed.

3. Security Features: This encompasses the specific security measures and functionalities implemented within the framework.

4. Interoperability Considerations: This final stage ensures the framework can work effectively with other systems and standards.

The arrows show how these components relate to each other:

i. Requirement Analysis informs both Security Features and Interoperability Considerations.
ii. Data management layer shapes the Interoperability Considerations.
iii. Security Features impact the Interoperability Considerations.

This framework design section provided a comprehensive approach to developing a secure and interoperable integration framework for M-Health services at the University of Nairobi Hospital. The structure covered the key areas necessary to ensure the successful implementation and operation of the framework.

4.5 Basic Pseudonymization Technique

Table 15 in the example below displays the real data, but after the pseudonymization process, the sensitive material is concealed, and the de-identified data is still significant and useful for research.

Table 20:Basic Pseudonymization technique

Healthcare ID	Date	Name	Medication	Condition
2001567898761234	12/12/2022	Babu Loliondo	Insulin	CD (Conduct Disorder)
2008123456785000	10/05/2022	John Pombe	Dapotum	MH (Malignant hyperthermia)
2001567898761234	10/10/2022	Babu Loliondo	Thalitone	CKD

Pseudonymization

Table 21:Pseudonymized data (Health care ID & Name)

HealthCare ID	Date	Name	Medication	Condition
0102	12/12/2022	A12	Insulin	CD(Conduct Disorder)
452	10/05/2022	B02	Dapotum	MH(Malignant hyperthermia)
2712	10/10/2022	N17	Thalitone	CKD

The data for the concealed connective index is kept on another computer or in a secure location that is inaccessible to regular users.

Table 22:Health ID, healthcare identifier Pseudonym

Healthcare ID	Healthcare Identifier Pseudonym
2001567898761234	0102
2008123456785000	452
2001567898761234	2712

Table 23:Name and name Pseudonym

Name	Name Pseudonym
Babu Loliondo	A12
John Pombe	B02
Babu Loliondo	N17

The distinction between encryption and pseudonymization is that sensitive information and relationships are exposed when encryption or password authorization is used. Pseudonymization, on the other hand, exposes relationships while concealing critical information. Data patterns must be preserved for linking or analysis, and personal data that will be shared—internally or with a partner—must be concealed while being used—are the two key conditions for Pseudonymization.

As a result, risk exposure will be lower, and any possible effects of internal and external security breaches will be lessened. Pseudonymization successfully makes stolen data unusable for identity theft and other types of fraud. By employing de-identified data to identify accounts, process account

papers, and record accounts, this makes secure outsourcing and offshore possible. The hospital can save money while greatly decreasing the security concerns associated with hiring third parties.

De-identified data can be used by system integrators, developers, and system administrators for the health software industry to estimate E-Health projects that deal with sensitive health data, design and test new systems that draw on existing operations for sensitive health data and maintain E-Health systems that manipulate sensitive data.

The Pseudonymization application(model) was developed using the C# programming language and database was created using the SQL server 2019, and the database management used was Microsoft SQL Server Management Studio.

4.6 Validation of the proposed framework

The objective of this study was to validate the proposed framework for improving the security of the E-Health system. To achieve this, a team of ten Information and Communication Technology (ICT) experts from the University of Nairobi was engaged. The experts were selected based on their expertise in cybersecurity and health informatics, and data was collected through a combination of structured interviews and detailed questionnaires. These experts were tasked with critically assessing both the theoretical soundness and the practical potential of the framework. The results of their evaluations were unanimous: all ten experts agreed that the implementation of the proposed framework would significantly enhance the security, reliability, and overall effectiveness of the E-Health system, thus ensuring better protection of sensitive patient data.

CHAPTER FIVE

5. SUMMARY ,CONCLUSIONS AND RECOMMENDATIONS.

5.1.Introduction

This chapter presents a summary of the recommendations and conclusions derived from the data analysis conducted in the study. It highlights the key findings and insights, offering a comprehensive overview of the outcomes in relation to the study's general objectives. Additionally, the chapter provides suggestions for further research, identifying areas where additional investigation could enhance understanding and contribute to the field. These recommendations are intended to guide future studies and support ongoing efforts to address the challenges and opportunities identified in the research.

5.2.Summary of findings

The results from this project revealed that over 70% believed that there is significance comprehensive security in the University Health systems.

It was established that a good number, over 60% of staff, had relative experience at the hospital for over 5years, and at least 75% of these have acquired relevant academic qualification diploma and above in the field of specialty.

On the issue of timely update of medical records, it was noted that if Electronic Health System Integration Framework for Secure M-Health Service, 65.90% of staff would find it helpful.

On the issue of protection of medical records data, the researcher noted that several security measures have been put in place for this, including rights and roles in level of access, offsite backup availability, anti-virus installation and IT support team in place with at least 65% basic IT knowledge provisioned.

Patient records have not been Pseudonymized, thus making information gathered to easily allow the individual to be directly identified.

The proposed framework was developed and validated by the ICT experts at the University of Nairobi Hospital. Therefore, the pseudonymization of the patient records will enhance the privacy of patient data that can be used in research purposes.

5.3.Conclusion

In conclusion, the objectives of this study were successfully achieved, highlighting the critical importance of a comprehensive information security framework for M-health systems at the University of Nairobi Hospital. The evaluation of current security measures underscored the necessity for robust protection mechanisms to safeguard sensitive health data. The design of a secure integration framework provides a structured approach to enhancing the security of M-health systems, ensuring that patient information is protected from potential threats. Finally, the validation of the proposed framework demonstrated its effectiveness in addressing the identified security challenges, thereby contributing to the overall improvement of the hospital's M-health systems. This work serves as a vital step towards ensuring that the University of Nairobi Hospital can confidently leverage M-health technologies while maintaining the highest standards of data security and patient confidentiality.

5.4.Future research recommendations

The introduction of EMR pseudonymization in the health system integration framework for secure M-health services in University of Nairobi Hospital is an enhanced solution that would improve in healthcare and associated policies frameworks to be revised and improved for better health services not only in the Hospital but in the country at large.

Based on the key findings the implications for practice include enhanced privacy protection for healthcare systems and this can be achieved by stronger data governance, access control mechanisms and secure data sharing. Furthermore, compliance with legal and ethical standards for healthcare services

A more focus should also address on expanding and integrating of similar systems and solutions deployed in other similar and blended environments and thus expand its usage in other hospitals in the country.

Explore and innovate possibilities to increase related services on the framework including simulations on some of the hospital activities that require similar facility in improving secure M-health. Suggestions for extending the research to cover new technologies such as Artificial Intelligence and blockchain.

REFERENCES

Adler-Milstein, J., & Jha, A. K. (2017). HITECH act drove large gains in hospital electronic health record adoption. *Health Affairs, 1;36*(8), 1416-1422.

Ahmed, I., & Mousa, A. (2016). Security and privacy issues in ehealthcare systems: Towards trusted services. *International Journal of Advanced Computer Science and Applications, 7*(9), 229–236.

Beebe, N. L. V. S. R. (2005). Using situational crime prevention theory to explain the effectiveness of information systems security. In *Proceedings of the 2005 SoftWars Conference* (pp. 1–18). Las Vegas, NV.

Bendiek, A., & Metzger, T. (2015). Deterrence theory in the cyber-century. In *Informatik 2015* (pp. 553–770). Bonn, Germany: Gesellschaft für Informatik e.V.

Bendiek, A., & Metzger, T. (2015). Deterrence theory in the cyber-century. *Working Paper, Research Division EU/Europe Stiftung Wissenschaft und Politik, German Institute for International and Security Affairs*.

Blumenthal, D. (2010). Launching HITECH. *New England Journal of Medicine, 362*(5), 382-385.

Bowman, S. (2013). Impact of electronic health record systems on information integrity: Quality and safety implications. *Perspectives in Health Information Management, 10*, 1c.

Brailer, D. J. (2005). Interoperability: The key to the future health care system. *Health Affairs, 24*(suppl1), W5-19-W5-21.

Brands, S. (2003). Privacy and security in electronic health. *Security*, 1–12.

Capra, F. (1997). *The web of life*. New York, NY: Doubleday-Anchor Books.

Charitoudi, K., & Blyth, A. (2013). A socio-technical approach to cyber risk management and impact assessment. *Journal of Information Security*, *4*(1), 33–41.

Chen, X., Zhang, Y., & Zhu, X. (2020)**.** *Security and Privacy in Electronic Medical Records: Theoretical Approaches and Practical Applications*. Journal of Healthcare Informatics, 15(2), 101–113

David, F. (2006). Mobile application security system. *Bell Labs Technical Journal, 11*(3).

Elkhodr, M., Shahrestani, S., & Kourouche, K. (2012). A proposal to improve the security of mobile banking applications. In *Proceedings of ICT and Knowledge Engineering* (pp. 260–265). IEEE.

Gejibo, S., Mancini, F., & Mughal, K. (2015). Mobile data collection: A security perspective. In A. Sasan (Ed.), *Mobile Health: A Technology Road Map* (pp. 1015–1042). Springer, Cham.

Goldstein, M. M., & Pewen, W. F. (2007). The imperative for privacy protections in the exchange of health information. *Health Affairs, 26*(3), 680-692

Gostin, L. O., Halabi, S. F., & Wilson, K. (2018). Health Data and Privacy in the Digital Era. *The Journal of the American Medical Association*, 320(3), 233–234.

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *Information & Computer Security, 21*(1), 69–79.

Ministry of Health, Government of Kenya. (2017). *Kenya Standards and Guidelines for mHealth Systems*.

Hong, K.S., Chi, Y.P., Chao, L. R., &Tang, J.H. (2003). An integrated system theory of information security management. Information Management & Computer Security, 11(5), 243–248

Innab, N. (2018). Availability, accessibility, privacy and safety issues facing electronic medical records. *International Journal of Security, Privacy and Trust Management, 7*(1), 01–10.

Iwaya, L.H., Ahmad, A., & Babar, M.A. (2020). Security and privacy for mHealth and uHealth systems: A systematic mapping study. *IEEE Access, 8,* 150081–150112.

Kellermann, A. L., & Jones, S. S. (2013). What it will take to achieve the as-yet-unfulfilled promises of health information technology. *Health Affairs, 32*(1), 63-68

Liddick, D. (2013). Techniques of neutralization and animal rights activists. *Deviant Behavior, 34*(8), 618–634.

Lizasoain, A., Tort, L. F., Garcia, M., Gomez, M. M., Leite, J. P., Miagostovich, M. P., Cristina, J., Colina, R., & Victoria, M. (2015). Environmental assessment reveals the presence of MLB-1 human astrovirus in Uruguay. *Journal of Applied Microbiology*, *119*, 859–867.

Lucas, J. (2013). Oracle: An introduction to the basics of data integrity enforcement in a variety of environments. *AMIS Technology Blog*.

Maranda, A., & Majchrzycka, A. (2016). Secure development model for mobile applications. *Bulletin of the Polish Academy of Sciences Technical Sciences*, *64*(3).

Ministry of Health. (2016). *Kenya National eHealth Policy, 2016-2030*.

Nganji, J. T., & Nggada, S. H. (2011). Disability-aware software engineering for improved system accessibility and usability. *International Journal of Software Engineering and Its Applications*, *5*(3), 47–62.

Nkosi, M., & Mekuria, F. (2010). Cloud computing for enhanced mobile health applications. *IEE*.

Pernebekova, A. P., & Ahbergenovich, B. A. (2015). Information security and the theory of unfaithful information. *Journal of Information Security*, *06*(04), 265–272.

Shifali, A., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health (mHealth) research.

Simplicio, M. A., Iwaya, L. H., Barros, B. M., Carvalho, T. C. M. B., & Naslund, M. (2015). Secourhealth: A delay-tolerant security framework for mobile health data collection. *IEEE Journal of Biomedical and Health Informatics*, *19*(2), 761-772.

Leon, N., Schneider, H., & Daviaud, E. (2012). Applying a framework for assessing the health system challenges to scaling up mHealth in South Africa. *BMC Medical Informatics and Decision Making, 12*, 123.

McCarthy, J., Kearney, P., & Butler, M. (2020). Data Integrity in Electronic Health Records: Ensuring Accuracy and Reliability. *International Journal of Health Information Systems*, 8(1), 45–59

O'Connor, M., Russell, D., & Finlay, R. (2019). Ensuring Availability in Critical Healthcare Information Systems: Best Practices. *Healthcare IT Journal*, 14(3), 98–105.

Salim, H., & Salim, H. M. (2014). A systems thinking and systems theory approach to managing cyber security risks. *Cyber Safety : A Systems Thinking and Systems Theory Approach*, (May).

Schein, R., Wilson, K., & Keelan, J. (2010). Literature review on effectiveness of the use of social media: A report for Peel Public Health. *Challenges, 129*(1), 63.

Serhani, M. A., Benharref, A., & Nujum, A. R. (2014). Intelligent remote health monitoring using evident-based DSS for automated assistance, 2674-7.

Shaikh, R. & Sasikala, P. (2019). Approaches to Enhancing Confidentiality in Healthcare Systems: Role-Based Access and Encryption. *Computers in Healthcare*, 12(2), 89–102.

Simplicio, M. A., Iwaya, L. H., Barros, B. M., Carvalho, T. C. M. B., & Naslund, M. (2015). Secourhealth: A delay-tolerant security framework for mobile health data collection. *IEEE Journal of Biomedical and Health Informatics, 19*(2), 761-772.

Tan, J., & Payton, F. C. (2010). Adaptive health management information systems: Concepts, cases, & practical applications (3rd ed.). Jones & Bartlett Learning.

Tarus, J. K., Gichoya, D., & Muumbo, A. (2015). Challenges of implementing e-learning in Kenya: A case of Kenyan public universities. *The International Review of Research in Open and Distributed Learning, 16*(1).

University of Nairobi. (2021, January 23). Fact file. Retrieved from https://uonbi.ac.ke/fact-file

Vimalachandran, P., Wang, H., Zhang, Y., & Whittaker, F. (2018). Ensuring data integrity in electronic health records: A quality healthcare implication.

Wallis, L., Blessing, P., Dalwai, M., & Shin, S. (2017). Integrating mHealth at point of care in low- and middle-income settings: The system perspective. *Global Health Action, 10*(00).

Wausi, A. N., & Waema, T. M. (2009). Organizational implementation of information systems innovations (Unpublished doctoral thesis). University of Nairobi, Kenya.

WHO. (2018). Use of appropriate digital technologies for public health (Vol. 28).

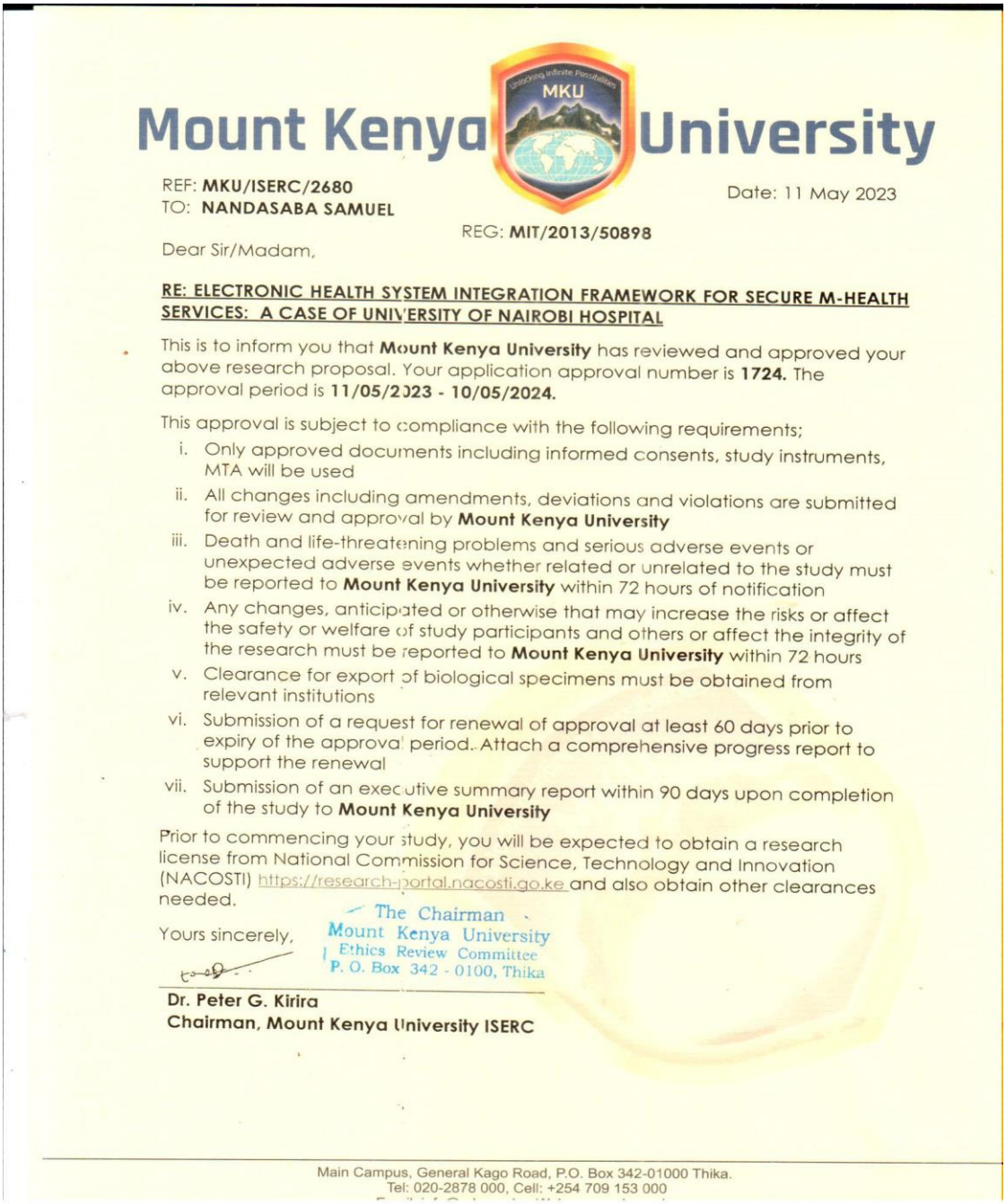
Li, W., & Cheng, L. (2013). Effects of neutralization techniques and rational choice theory on Internet abuse in the workplace. Paper presented at the Pacific Asia Conference on Information Systems, Jeju Island, Korea.

Zdravkova, V. (2015). Identity management approach in Internet of Things. Aalborg University.

Zhou, Y., Liu, Z., & Wang, H. (2019). Privacy and Security Frameworks for Electronic Medical Records. *Cybersecurity in Healthcare Journal*, 6(4), 287–301.

APPENDICES

i. Ethics review committee Certificate.



Mount Kenya University

REF: **MKU/ISERC/2680**
TO: **NANDASABA SAMUEL**

Date: 11 May 2023

REG: **MIT/2013/50898**

Dear Sir/Madam,

RE: ELECTRONIC HEALTH SYSTEM INTEGRATION FRAMEWORK FOR SECURE M-HEALTH SERVICES: A CASE OF UNIVERSITY OF NAIROBI HOSPITAL

This is to inform you that **Mount Kenya University** has reviewed and approved your above research proposal. Your application approval number is **1724.** The approval period is **11/05/2023 - 10/05/2024.**

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 **Mount Kenya University**
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 **Mount Kenya University** within 72 hours of notification
iv. Any changes, anticipated or otherwise that may increase the risks or affect the safety or welfare of study participants and others or affect the integrity of the research must be reported to **Mount Kenya University** 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 **Mount Kenya University**

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.

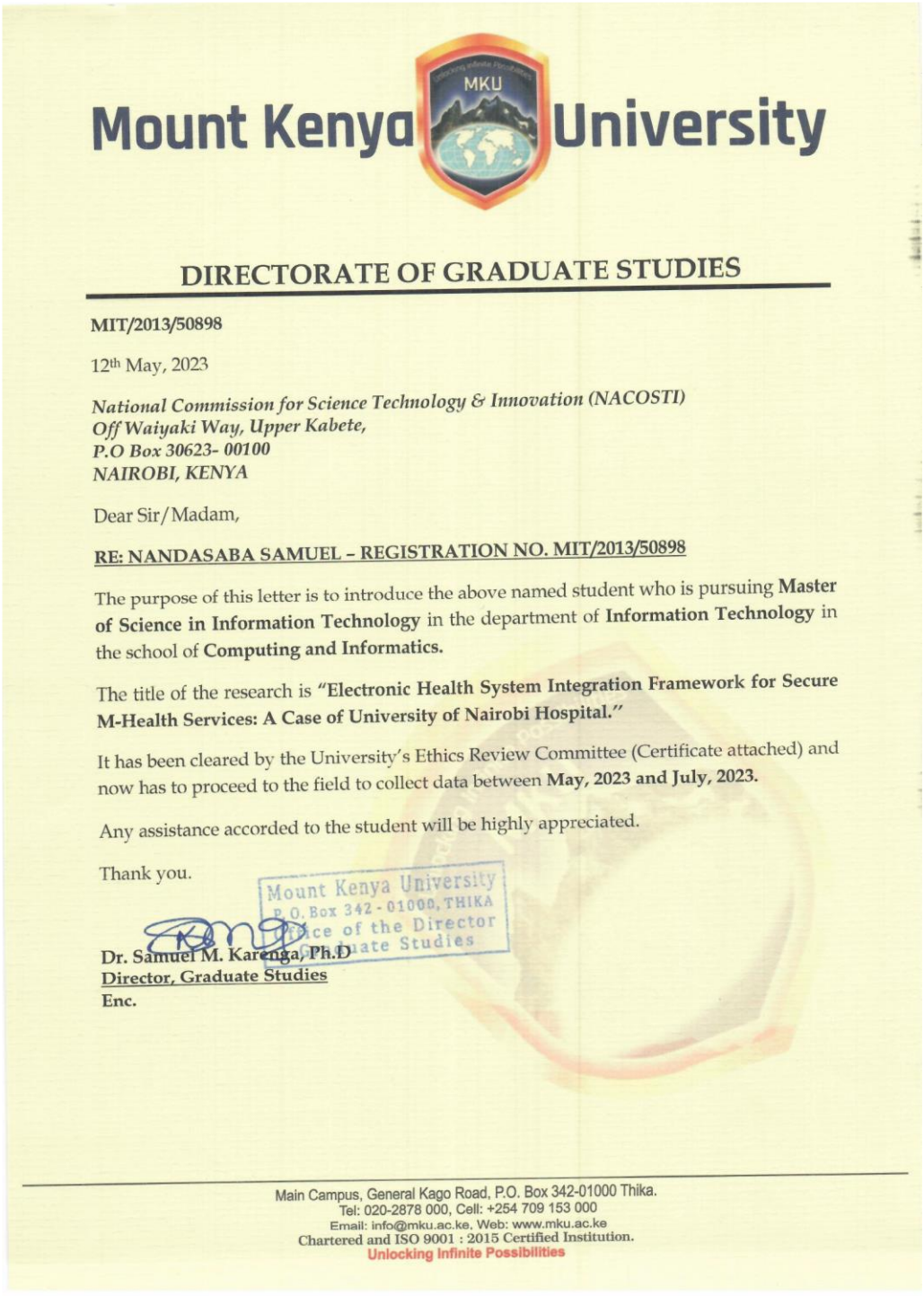
Yours sincerely,

The Chairman
Mount Kenya University
Ethics Review Committee
P. O. Box 342 - 0100, Thika

Dr. Peter G. Kirira
Chairman, Mount Kenya University ISERC

Main Campus, General Kago Road, P.O. Box 342-01000 Thika.
Tel: 020-2878 000, Cell: +254 709 153 000

ii. Introduction Letter from postgraduate



Mount Kenya University

MKU

DIRECTORATE OF GRADUATE STUDIES

MIT/2013/50898

12th May, 2023

National Commission for Science Technology & Innovation (NACOSTI)
Off Waiyaki Way, Upper Kabete,
P.O Box 30623- 00100
NAIROBI, KENYA

Dear Sir/Madam,

RE: NANDASABA SAMUEL – REGISTRATION NO. MIT/2013/50898

The purpose of this letter is to introduce the above named student who is pursuing **Master of Science in Information Technology** in the department of **Information Technology** in the school of **Computing and Informatics.**

The title of the research is **"Electronic Health System Integration Framework for Secure M-Health Services: A Case of University of Nairobi Hospital."**

It has been cleared by the University's Ethics Review Committee (Certificate attached) and now has to proceed to the field to collect data between **May, 2023 and July, 2023.**

Any assistance accorded to the student will be highly appreciated.

Thank you.

Mount Kenya University
P.O. Box 342 - 01000, THIKA
Office of the Director
Graduate Studies

Dr. Samuel M. Karenga, Ph.D
Director, Graduate Studies
Enc.

Main Campus, General Kago Road, P.O. Box 342-01000 Thika.
Tel: 020-2878 000, Cell: +254 709 153 000
Email: info@mku.ac.ke, Web: www.mku.ac.ke
Chartered and ISO 9001 : 2015 Certified Institution.
Unlocking Infinite Possibilities

iii. Approved certificate from NACOSTI.

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY & INNOVATION

Ref No: **701067**

Date of Issue: **25/May/2023**

RESEARCH LICENSE

This is to Certify that Mr.. Samuel Nandasaba of Mount Kenya University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: ELECTRONIC HEALTH SYSTEM INTEGRATION FRAMEWORK FOR SECURE M-HEALTH SERVICES: A CASE OF UNIVERSITY OF NAIROBI HOSPITAL for the period ending : 25/May/2024.

License No: **NACOSTI/P/23/26102**

701067

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.

See overleaf for conditions

iv. Informed Consent form

ELECTRONIC HEALTH INTEGRATION FRAMEWORK FOR SECURE M-HEALTH SERVICES: CASE OF UNIVERSITY OF NAIROBI HOSPITAL

Dear Participant,

I invite you to participate in a research study entitled **Electronic Health integration System framework for Secure M-Health services: A Case study of University of Nairobi Hospital.** I am currently enrolled in the MSc. In IT at Mount Kenya University and am in the process of writing my master's thesis. The purpose of the research seeks to propose a framework for E health integration for secure M-health services. The enclosed questionnaire has been designed to collect information on system security (Confidentiality, Availability and Integrity). Your participation in this research project is completely voluntary. You may decline altogether or leave blank any questions you don't wish to answer. There are no known risks to participation beyond those encountered in everyday life. Your responses will remain confidential and anonymous. Data from this research will be kept under lock and key and reported only as a collective combined total. No one other than the researchers will know your individual answers to this questionnaire. There are no direct benefits to you for participating in this research. However, you may find it interesting to talk about the issues addressed in the research and it may be beneficial to the field and to future clients or individuals who have experienced similar concerns

If you agree to participate in this project, please answer the questions on the questionnaire as best you can. It should take approximately fifteen minutes to complete. Please return the questionnaire as soon as possible to enable me to complete the project report.

If you have any questions about this project, feel free to contact *the INVESTIGATOR*, (*Nandasaba Samuel, nandasaba.sam@gmail.com*). If you have questions about your rights as a research participant, please be in touch with the Chairman, Mount Kenya University, Ethical Review Committee, P.O Box 342-01000, Thika.

Thank you for your assistance in this important endeavor.

CONSENT

I have read, and I understand the information provided and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I understand that I will be given a copy of this consent form. I voluntarily agree to take part in this study.

Participant's signature _____ Date _____

Investigator's signature _____ Date _____

v. Interview Schedule

Preamble: Permission to record

Copyright waiver

Section 1- Introduction

i. Which role do you have in the university hospital?

ii. What are your main responsibilities in the system?

iii. How long have you worked within the Hospital?

iv. What is the highest level of your education?

Section 2- CIA triad system implemented at the site of study.

The researcher used open-ended questions to gain more information on the CIA of the system implemented at the site of study.

1. Do the developers of the system comply with the integrity attributes?
2. Which measures have been used to ensure the availability of the system?
3. Is training conducted to the system users to know the current security threats?
4. Which measures have been implemented in the system to ensure patient data confidentiality?

vi. Questionnaire

I am a master's student at Mt. Kenya University in my initial stages of preparing a Research project. The information gotten herein will be used to enhance the security of many Mobile health Applications that are coming up.

I kindly request you to sacrifice 10 to 15 minutes of your precious time to complete this questionnaire. Kindly complete the questionnaire as truthfully as possible.

Your privacy and confidentiality are guaranteed as you participate in this study. The information provided herein will be treated with utmost confidence and will only be used for the purpose of this research.

SYSTEM INFORMATION SECURITY

Section A: General Information

1. Please indicate your position in the hospital (Optional)

   ---

2. Please indicate your gender. Male [ ] Female [ ]

3. Please indicate which department you work in

   Casualty [ ] Laboratory [ ] ICT [ ]

   Pharmacy [ ] Surgery [ ] Maternity Ward [ ]

   Pediatric Ward [ ]

   Other ---

4. How long have you worked in this Hospital?

   Less than 5 years [ ] 5-10 years[ ] 10-20 years[ ] over 20 years[ ]

5. What is your highest academic qualification?

   Certificate [ ] Diploma [ ]

   Graduate [ ] Masters [ ]

In a 5-point scale where: 1 – Strongly disagree (SD) 2 – Disagree (DS), 3 – Neutral (NT) 4 – Agree (AG) - Strongly agree (SA).

No.	Item	SD	DS	NT	A	SA
6.	The Hospital ensures all actors add the medical records as soon they are through with the patient to ensure completeness and reliability.	1	2	3	4	5
7.	The patient's records are continuously updated as soon as there are changes to ensure reliability.	1	2	3	4	5
8.	The hospital ensures accuracy of medical records by protecting the information against losses	1	2	3	4	5
9.	The hospital ensures the medical records are protected against distortion while transmitting through electronic media	1	2	3	4	5
10.	The hospital ensures that the employees have basic IT knowledge to key in accurate data.	1	2	3	4	5
11.	Passwords have been put in computers for protection of data	1	2	3	4	5

12.	The hospital has ensured that the system has various users with different roles to avoid unauthorized access of patients data	1	2	3	4	5
13.	The Application system always up and running.	1	2	3	4	5
14.	The flow of Information in the application system traceable through logging and documentation.	1	2	3	4	5
15.	There is an offsite backup of the patient data	1	2	3	4	5
No.	**Item**	**SD**	**DS**	**NT**	**A**	**SA**
17.	Healthcare professionals have access to patients Information when needed.	1	2	3	4	5
18.	The computer being used has an updated antivirus	1	2	3	4	5
19.	Patient records are always Pseudonymized	1	2	3	4	5

Kindly indicate the extent to which application of information security strategies has impacted Security of M-health in the hospital.

In a 5-point scale where: 1 – Strongly disagree (SD) 2 – Disagree (DS), 3 – Neutral (NT) 4 – Agree (AG) - Strongly agree (SA).

No.	**Indicator**	**SD**	**DS**	**NT**	**A**	**SA**
20.	Patients' medical records are easily retrieved from the information systems when needed.					

21	There is better patients' medication management due to availability of information					
22	There is improved and accurate clinical decisions					
23	Medical history information is available to avoid duplication of diagnostic imaging and testing.					
24	There is improved and accurate clinical decisions					

vii. Turnitin Report

ELECTRONIC HEALTH SYSTEMINTEGRATION FRAMEWORK FOR SECURE M-HEALTH SERVICES: A CASE OF UNIVERSITY OF NAIROBI HOSPITAL

by Nandasaba Samuel

Submission date: 21-Aug-2023 10:31AM (UTC+0300)

Submission ID: 2148781653

File name: Nandasaba-Thesis_-_turnitin.docx (1.3M)

Word count: 10962

Character count: 63210

ELECTRONIC HEALTH SYSTEM INTEGRATION FRAMEWORK FORSECURE M-HEALTH SERVICES: A CASE OF UNIVERSITY OF NAIROBI HOSPITAL

ORIGINALITY REPORT

14%	11%	5%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1 erepository.uonbi.ac.ke
Internet Source

2 Submitted to University of Nairobi
Student Paper

3 Submitted to Eastern Mediterranean University
Student Paper

4 A. Majchrzycka, A. Poniszewska-Marańda. "Secure development model for mobile applications", Bulletin of the Polish Academyof Sciences Technical Sciences, 2016
Publication

5 David Floyd. "Mobile application security system (MASS)", Bell Labs Technical Journal, 2006
Publication

6 Springer Series in Bio-/Neuroinformatics, 2015.
Publication

2%	
1%	
1%	
1%	
<1%	
<1%	

ELECTRONIC HEALTH SYSTEM INTEGRATION FRAMEWORK FORSECURE M-HEALTH SERVICES: A CASE OF UNIVERSITY OF NAIROBI HOSPITAL

GRADEMARK REPORT FINAL GRADE

/100

PAGE 1

viii. Pseudonymization code

```
<%@ Page Language="C#" Title="PID_Create" MasterPageFile="~/pages/Main.Master" AutoEventWireup="true" CodeBehind="NewPatient.aspx.cs" Inherits="Prac.pages.NewPatient" %>

<asp:Content ID="Content1" ContentPlaceHolderID="Main1" runat="Server">
   <!-- Content Wrapper. Contains page content -->
   <div class="content-wrapper">
      <!-- Content Header (Page header) -->
      <section class="content-header">
        <h1>Patient ID
            <%--<small>Version 2.0</small>--%>
         </h1>
         <ol class="breadcrumb">
            <li><a href="Dashboard.aspx"><i class="fa fa-dashboard"></i>Home</a></li>
            <li class="active">Create PID</li>
         </ol>
      </section>
      <!-- Main content -->
      <section class="content">
         <div class="row">
            <div class="col-md-12">
               <asp:MultiView ID="MultiView1" runat="server">
```

```
<asp:View ID="View1" runat="server">
    <div class="box box-warning box-solid">
        <div class="box-header with-border">
            <h3 class="box-title">New PID</h3>
        </div>
        <div class="box-body">
            <table class="table">
                <thead>
                    <tr>
                        <th></th>
                        <th></th>
                        <th></th>
                        <th>
                            <asp:LinkButton ID="LinkButton1" ToolTip="Print" class="fa fa-plus-square pull-right" runat="server"></asp:LinkButton></th>
                    </tr>
                </thead>
                <tbody>
                    <tr>
                        <th>No:</th>
                        <td>
                            <asp:Label ID="lblNo" runat="server"></asp:Label>
```

```
                    </td>
                    <th>Date:</th>
                    <td>
                        <asp:Label ID="lbldate" runat="server"></asp:Label>
                    </td>
                </tr>
                <tr>
                    <%--<th>Responsibility Centre:</th>
                    <td>
                        <asp:DropDownList ID="ddlresponibilitycentres" runat="server" CssClass="form-control select2"></asp:DropDownList>
                    </td>--%>
                    <th>Ombudsman Id:</th>
                    <td>
                        <asp:Label ID="lbluserId" runat="server" Text="User Id" CssClass="text-info"></asp:Label></td>
                </tr>
                <tr>
                    <th>Patient ID: </th>
                    <td colspan="3">
                        <asp:TextBox ID="txtpatientid" runat="server" CssClass="form-control" TextMode="MultiLine"></asp:TextBox></td>
                    <th>Name: </th>
```

```
                    <td colspan="3">

                        <asp:TextBox ID="txtname" runat="server" CssClass="form-control" TextMode="MultiLine"></asp:TextBox></td>

                    </tr>

                    <tr>

                        <th>Condition: </th>

                        <td colspan="3">

                            <asp:TextBox ID="txtcomplaindesc" runat="server" CssClass="form-control" TextMode="MultiLine"></asp:TextBox></td>

                        <th>Medication: </th>

                        <td colspan="3">

                            <asp:TextBox ID="txtHdescription" runat="server" CssClass="form-control" TextMode="MultiLine"></asp:TextBox></td>

                        <th></th>

                        <td></td>

                    </tr>

                    <tr>

                        <th>Date:</th>

                        <td>

                            <asp:TextBox ID="dtDate" CssClass="form-control" runat="server" Width="350px"></asp:TextBox>

                            <script>

                                $j('#Main1_dtDate').Zebra_DatePicker({
```

```
                    // remember that the way you write down dates
                    // depends on the value of the "format" property!
                    //direction: [1, false],
                    //disabled_dates: ['* * * 0,6']
                });</script>
            </td>
            <th></th>
            <td></td>
            <td></td>
            <td>
                <asp:Button ID="btnSubmit" class="btn btn-primary pull-right" runat="server" Text="Submit" OnClick="btnSubmit_Click" /></td>
            </tr>
        </tbody>
    </table>
</div>
</div>
</asp:View>
</asp:MultiView>
</div>
</div>
</section>
```

```
    </div>
</asp:Content>

//CODE BEHIND FILE
using System;
using System.Collections;
using System.Collections.Generic;
using System.Data;
using System.Data.SqlClient;
using System.Linq;
using System.Web;
using System.Web.UI;
using System.Web.UI.WebControls;

namespace Prac.pages
{
    public partial class NewPatient : System.Web.UI.Page
    {
        protected void Page_Load(object sender, EventArgs e)
        {
            if (!IsPostBack)
```

```
    {
        if (Session["username"] == null)
        {
            Response.Redirect("~/Default.aspx");
        }
        else
        {
            MultiView1.ActiveViewIndex = 0;
            lblNo.Text = GenerateRandomString(5);//Generated random string
            lbluserId.Text = lblNo.Text;
            //lbldate.Text = DateTime.Today();
        }
    }
}

private void Message(string p)
{
    string strScript = null;
    strScript = "<script>";
    strScript = strScript + "alert('" + p + "');";
    strScript = strScript + "</script>";
```

```
        Page.RegisterStartupScript("ClientScript", strScript.ToString());
    }
```

//This method is used to generate the random pseudonym characters using a collection of Numbers and Capital letters as shown below

```
    public static string GenerateRandomString(int length)
    {
        const string chars = "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";
        var random = new Random();
        return new string(Enumerable.Repeat(chars, length)
          .Select(s => s[random.Next(s.Length)]).ToArray());
    }
    protected void btnSubmit_Click(object sender, EventArgs e)
    {
        try
        {
            //Collect data
            string pid = txtpatientid.Text;
            string pname = txtname.Text;
            string patientid = lblNo.Text;
            string CreatedDate = "";// lbldate.Text;
            string pseudoz = GenerateRandomString(8) + " " + GenerateRandomString(8);
            string complain = txtHdescription.Text.ToString().Replace("'", "");
```

```
string complaindesc = txtcomplaindesc.Text.ToString().Replace("'", "");
DateTime datedv = Convert.ToDateTime(dtDate.Text);
#region CreatePID
using (SqlConnection connToNAV = MyComponents.getconnToNAV())
{
   string sqlStmt = null;
   sqlStmt = "spInsertPatientData";
   SqlCommand cmd = new SqlCommand();
   cmd.CommandText = sqlStmt;
   cmd.Connection = connToNAV;
   cmd.CommandType = CommandType.StoredProcedure;
   cmd.Parameters.AddWithValue("@patid", "'" + pid + "'");
   cmd.Parameters.AddWithValue("@pname", "'" + pname + "'");
   cmd.Parameters.AddWithValue("@PID", "'" + patientid + "'");
   cmd.Parameters.AddWithValue("@datedv", "'" + datedv + "'");
   cmd.Parameters.AddWithValue("@pseudo", "'" + pseudoz + "'");
   cmd.Parameters.AddWithValue("@Complain", "'" + complain + "'");
   cmd.Parameters.AddWithValue("@Compdesc", "'" + complaindesc + "'");
   cmd.ExecuteNonQuery();
   {
      //SqlCommand cmd = new SqlCommand(query, connToNAV)
```

```
            string sqlStmts = null;
            SqlCommand cmd2 = new SqlCommand(sqlStmts, connToNAV);
            sqlStmts = "spInsertPatients";
            cmd2.CommandText = sqlStmts;
            cmd2.Connection = connToNAV;
            cmd2.CommandType = CommandType.StoredProcedure;
            cmd2.Parameters.AddWithValue("@patid", "'" + pid + "'");
            cmd2.Parameters.AddWithValue("@pname", "'" + pname + "'");
            cmd2.Parameters.AddWithValue("@PID", "'" + patientid + "'");
            cmd2.Parameters.AddWithValue("@pseudo", "'" + pseudoz + "'");
            cmd2.ExecuteNonQuery();
            //UpdateApplicationNo(patientid, connToNAV);
        }
        //UpdateApplicationNo(patientid, connToNAV);
    }

    Message("Hello " + pid + " Your Patient was recorded successfully");
    Response.Redirect("NewListing.aspx");
}
catch (Exception Ex)
{
```

```
            Message("Error");
            Response.Redirect("NewListing.aspx");
            //cSite.SendErrorToDeveloper(Ex);
            Ex.Data.Clear();
        }
        #endregion
    }
  }
}
```

```
<%@ Page Title="About" Language="C#" MasterPageFile="~/Site.Master" AutoEventWireup="true" CodeBehind="About.aspx.cs" Inherits="Prac.About" %>

<asp:Content ID="BodyContent" ContentPlaceHolderID="MainContent" runat="server">
    <h2><%: Title %>.</h2>
    <h3>Your application description page.</h3>
    <p>Use this area to provide additional information.</p>
</asp:Content>
```

```
<%@ Page Title="Contact" Language="C#" MasterPageFile="~/Site.Master" AutoEventWireup="true" CodeBehind="Contact.aspx.cs" Inherits="Prac.Contact" %>
```

```
<asp:Content ID="BodyContent" ContentPlaceHolderID="MainContent" runat="server">
    <h2><%: Title %>.</h2>
    <h3>Your contact page.</h3>
    <address>
        One Microsoft Way<br />
        Redmond, WA 98052-6399<br />
        <abbr title="Phone">P:</abbr>
        425.555.0100
    </address>

    <address>
        <strong>Support:</strong>   <a href="mailto:Support@example.com">Support@example.com</a><br />
        <strong>Marketing:</strong>   <a href="mailto:Marketing@example.com">Marketing@example.com</a>
    </address>
</asp:Content>
<%@ Page Title="Login" Language="C#" MasterPageFile="~/Site.Master" AutoEventWireup="true" CodeBehind="Default.aspx.cs" Inherits="Prac._Default" %>
<asp:Content ID="BodyContent" ContentPlaceHolderID="MainContent" runat="server">

    <div class="box box-success">
        <div class="box-header with-border">
```

```
        <img src="images/logo.png" class="img-responsive text-center" style="width:290px;padding-left:160px" alt="User Image"/>

        <center>

   <a href="#" style="font-family:monotype-corsiva; font-size:30px; color:#046CAB"><strong>PraC </strong></a>

 </center>

        <%--<p class="login-box-msg">Sign in to start your session</p>--%>

      </div>

      <!-- /.box-header -->

      <!-- form start -->

      <div class="form-horizontal">

        <div class="box-body">

          <asp:Label ID="LblError" runat="server" CssClass="label label-danger"></asp:Label>

          <div class="form-group">

            <label for="inputEmail3" class="col-sm-2 control-label">Username</label>



            <div class="col-sm-10">

              <asp:TextBox ID="txtusername" class="form-control" placeholder="Admin Number" type="email" runat="server"></asp:TextBox>

              <%--<input type="email" class="form-control" id="inputEmail3" placeholder="Email">--%>

            </div>

          </div>
```

```
<div class="form-group">
    <label for="inputPassword3" class="col-sm-2 control-label">Password</label>

    <div class="col-sm-10">
        <asp:TextBox ID="txtpassword" class="form-control" placeholder="Password" type="password" runat="server"></asp:TextBox>
        <%--<input type="password" class="form-control" id="inputPassword3" placeholder="Password">--%>
    </div>
</div>
<div class="form-group">
    <div class="col-sm-offset-2 col-sm-10">
        <div class="checkbox">
            <label>
                <input type="checkbox">
                Remember me

            </label>
        </div>
    </div>
</div>
</div>
```

```
        <!-- /.box-body -->

        <div class="box-footer">

            <asp:LinkButton ID="lbtnForgot" type="submit" class="btn btn-warning" runat="server" OnClick="lbtnForgot_Click">Forgot Password?</asp:LinkButton>

            <asp:LinkButton ID="LbtnLogin" type="submit" class="btn btn-success pull-right" runat="server" OnClick="btnLogin_Click">Sign in</asp:LinkButton>

        </div>

        <!-- /.box-footer -->

      </div>

   </div>

</asp:Content>



<%@ Master Language="C#" AutoEventWireup="true" CodeBehind="Site.master.cs" Inherits="Prac.SiteMaster" %>



<!DOCTYPE html>

<html>

<head runat="server">

  <meta charset="utf-8">

  <meta http-equiv="X-UA-Compatible" content="IE=edge">

  <title>PraC | <%: Page.Title %></title>

    <link rel="shortcut icon" href="images/logo.png" />

  <!-- Tell the browser to be responsive to screen width -->
```

```
<meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">

<!-- Bootstrap 3.3.7 -->

<link rel="stylesheet" href="bower_components/bootstrap/dist/css/bootstrap.min.css">

<!-- Font Awesome -->

<link rel="stylesheet" href="bower_components/font-awesome/css/font-awesome.min.css">

<!-- Ionicons -->

<link rel="stylesheet" href="bower_components/Ionicons/css/ionicons.min.css">

<!-- Theme style -->

<link rel="stylesheet" href="dist/css/AdminLTE.min.css">

<!-- iCheck -->

<link rel="stylesheet" href="plugins/iCheck/square/blue.css">


<!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and media queries -->

<!-- WARNING: Respond.js doesn't work if you view the page via file:// -->

<!--[if lt IE 9]>

<script src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js"></script>

<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>

<![endif]-->


<!-- Google Font -->
```

```
  <link                                                                    rel="stylesheet"
href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,600,700,300italic,400ital
ic,600italic">

</head>

<body class="hold-transition login-page">

    <form runat="server">

<div class="login-box">




  <!-- /.login-logo -->

    <asp:ContentPlaceHolder ID="MainContent" runat="server">

          </asp:ContentPlaceHolder>



  <!-- /.login-box-body -->

</div>

<!-- /.login-box -->



<!-- jQuery 3 -->

<script src="bower_components/jquery/dist/jquery.min.js"></script>

<!-- Bootstrap 3.3.7 -->

<script src="bower_components/bootstrap/dist/js/bootstrap.min.js"></script>

<!-- iCheck -->
```

```
<script src="plugins/iCheck/icheck.min.js"></script>
<script>
   $(function () {
      $('input').iCheck({
         checkboxClass: 'icheckbox_square-blue',
         radioClass: 'iradio_square-blue',
         increaseArea: '20%' /* optional */
      });
   });
</script>
      </form>
</body>
</html>
```

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Web;
using System.Web.Routing;
using System.Web.UI;
```

```
using System.Web.UI.WebControls;
using Microsoft.AspNet.FriendlyUrls.Resolvers;

namespace Prac
{
    public partial class ViewSwitcher : System.Web.UI.UserControl
    {
        protected string CurrentView { get; private set; }

        protected string AlternateView { get; private set; }

        protected string SwitchUrl { get; private set; }

        protected void Page_Load(object sender, EventArgs e)
        {
            // Determine current view
            var isMobile = WebFormsFriendlyUrlResolver.IsMobileView(new HttpContextWrapper(Context));
            CurrentView = isMobile ? "Mobile" : "Desktop";

            // Determine alternate view
            AlternateView = isMobile ? "Desktop" : "Mobile";
```

```
        // Create switch URL from the route, e.g. ~/__FriendlyUrls_SwitchView/Mobile?ReturnUrl=/Page
        var switchViewRouteName = "AspNet.FriendlyUrls.SwitchView";
        var switchViewRoute = RouteTable.Routes[switchViewRouteName];
        if (switchViewRoute == null)
        {
            // Friendly URLs is not enabled or the name of the switch view route is out of sync
            this.Visible = false;
            return;
        }
        var url = GetRouteUrl(switchViewRouteName, new { view = AlternateView, __FriendlyUrls_SwitchViews = true });
        url += "?ReturnUrl=" + HttpUtility.UrlEncode(Request.RawUrl);
        SwitchUrl = url;
      }
   }
}
<?xml version="1.0" encoding="utf-8"?>
<!-- For more information on using web.config transformation visit https://go.microsoft.com/fwlink/?LinkId=125889 -->

<configuration xmlns:xdt="http://schemas.microsoft.com/XML-Document-Transform">
```

```
<!--
  In the example below, the "SetAttributes" transform will change the value of
  "connectionString" to use "ReleaseSQLServer" only when the "Match" locator
  finds an attribute "name" that has a value of "MyDB".

  <connectionStrings>
    <add name="MyDB"
      connectionString="Data Source=ReleaseSQLServer;Initial Catalog=MyReleaseDB;Integrated Security=True"
      xdt:Transform="SetAttributes" xdt:Locator="Match(name)"/>
  </connectionStrings>
-->
<system.web>
  <!--
    In the example below, the "Replace" transform will replace the entire
    <customErrors> section of your web.config file.
    Note that because there is only one customErrors section under the
    <system.web> node, there is no need to use the "xdt:Locator" attribute.
        <customErrors defaultRedirect="GenericError.htm"
      mode="RemoteOnly" xdt:Transform="Replace">
      <error statusCode="500" redirect="InternalError.htm"/>
    </customErrors>
```

```
    -->
  </system.web>
</configuration>
<%@ Page Language="C#" Title="_Complain" MasterPageFile="~/pages/Main.Master" AutoEventWireup="true" CodeBehind="Complain.aspx.cs" Inherits="Prac.pages.Complain" %>

<asp:Content ID="Content1" ContentPlaceHolderID="Main1" runat="Server">
    <!-- Content Wrapper. Contains page content -->
    <div class="content-wrapper">
        <!-- Content Header (Page header) -->
        <section class="content-header">
            <h1>Anonymous Complain
                <%--<small>Version 2.0</small>--%>
            </h1>
            <ol class="breadcrumb">
                <li><a href="Dashboard.aspx"><i class="fa fa-dashboard"></i>Home</a></li>
                <li class="active">Raise Complain</li>
            </ol>
        </section>
```

```
<%@ Page Language="C#" MasterPageFile="~/pages/Main.Master" Title="Dashboard" AutoEventWireup="true" CodeBehind="Dashboard.aspx.cs" Inherits="Prac.pages.Dashboard" %>

<asp:Content ID="Content1" ContentPlaceHolderID="Main1" runat="Server">

    <!-- Content Wrapper. Contains page content -->

    <div class="content-wrapper">

        <!-- Content Header (Page header) -->

        <section class="content-header">

            <h1 style="font-family:monotype-corsiva">Dashboard


                <%--<small>Version 2.0</small>--%>

            </h1>

            <div class="row">

                <div class="col-md-12">

                    <div class="box">

                        <div class="box-header with-border">

                            <h3 class="box-title">User Profile</h3>


                            <div class="box-tools pull-right">

                                <button type="button" class="btn btn-box-tool" data-widget="collapse">

                                    <i class="fa fa-minus"></i>

                                </button>

                                <div class="btn-group">
```

```
                    <button type="button" class="btn btn-box-tool dropdown-toggle" data-toggle="dropdown">
                      <i class="fa fa-wrench"></i>
                    </button>
                    <ul class="dropdown-menu" role="menu">
                      <%-- <li><a href="#">Action</a></li>
                      <li><a href="#">Another action</a></li>
                      <li><a href="#">Something else here</a></li>
                      <li class="divider"></li>
                      <li><a href="#">Separated link</a></li>--%>
                    </ul>
                  </div>
                  <button type="button" class="btn btn-box-tool" data-widget="remove"><i class="fa fa-times"></i></button>
                </div>
              </div>
              <!-- /.box-header -->
              <div class="box-body">
                <div class="row">
                  <!-- /.col -->
                  <div class="col-md-4">
                    <p class="text-center">
```

```
                    <strong>Personal Information </strong>

                </p>

                <div class="box-body box-profile">

                    <asp:Image ID="ImgProfileDefault" class="profile-user-img img-responsive img-circle" runat="server" Height="250px" Width="200px" Visible="false" alt="User profile picture" />

                    <asp:Image ID="ImgProfilePic" class="profile-user-img img-responsive img-circle" runat="server" Height="250px" Width="200px" alt="User profile picture" />

                    <%--<img class="profile-user-img img-responsive img-circle" src="../../dist/img/user4-128x128.jpg" alt="User profile picture">--%>

                    <h3 class="profile-username text-center">

                      <asp:Label ID="LblTitle" runat="server" Text="" Visible="false"></asp:Label>

                      <asp:Label ID="LblAdminName" runat="server" Text=""></asp:Label></h3>

                    <p class="text-muted text-center">

                      <asp:Label ID="LblDesignation" runat="server" Text=""></asp:Label></p>

                    <%--<a href="#" class="btn btn-primary btn-block"><b>Follow</b></a>--%>

                </div>

                <div class="progress-group">

                  <span class="progress-text"></span>

                  <span class="progress-number"><b></b></span>
```

```
                    <div class="progress sm">
                        <div class="progress-bar progress-bar-green" style="width: 100%"></div>
                    </div>
                </div>
            </div>
            <!-- /.col -->
            <div class="col-md-8">
                <p class="text-center">
                    <strong>-</strong>
                </p>

                <ul class="list-group list-group-unbordered">
                    <%--<li class="list-group-item">
                        <b>--:</b> <a class="pull-right">
                            <asp:Label ID="LblEmployeeNo" runat="server" Text=""></asp:Label></a>
                    </li>
                    <li class="list-group-item">
                        <b>--:</b> <a class="pull-right">
                            <asp:Label ID="LblIDNo" runat="server" Text=""></asp:Label></a>
                    </li>--%>
```

```
<%--<li class="list-group-item">
   <b>Full Name:</b> <a class="pull-right">
      </a>
</li>--%>
<%--<li class="list-group-item">
   <b>Job Title:</b> <a class="pull-right"></a>
</li>--%>
<li class="list-group-item">
   <b>--:</b> <a class="pull-right">
      <asp:Label ID="lblEmail" runat="server" Text=""></asp:Label></a>
</li>
</ul>
<div class="box-footer clearfix">
<li class="dropdown">
<a href="#" class="dropdown-toggle btn btn-sm btn-success btn-flat pull-left" data-toggle="dropdown">Options<span class="caret"></span></a>
<ul class="dropdown-menu" role="menu">
<li><a href="NewListing.aspx" class="fa fa-hand-o-right">View Records</a></li>
   <li class="divider"></li>
   <li><a href="PatientsListing.aspx"><i class="fa fa-hand-o-right"></i>All Patients</a></li>
</ul>
```

```
                    </li>
                        <a href="Changepassword.aspx" class="btn btn-sm btn-default btn-flat pull-right">Change password</a>
                    </div>
                </div>
            </div>
            <!-- /.row -->
        </div>
    </div>
    <!-- /.box -->
</div>
<!-- /.col -->
</div>
</section>
<!-- /.content -->
</div>
<!-- /.content-wrapper -->
</asp:Content>
<!-- Main content -->
<section class="content">
<div class="row">
<div class="col-md-12">
```

```
<asp:MultiView ID="MultiView1" runat="server">
    <asp:View ID="View1" runat="server">
        <div class="box box-warning box-solid">
            <div class="box-header with-border">
                <h3 class="box-title">New PID</h3>
            </div>
            <div class="box-body">
                <table class="table">
                    <tbody>
                        <tr>
                            <th>Patient ID: </th>
                            <td colspan="3">
                                <asp:TextBox ID="txtpatientid" runat="server" CssClass="form-control" TextMode="MultiLine"></asp:TextBox></td>
                            <th>Name: </th>
                            <td colspan="3">
                                <asp:TextBox ID="txtname" runat="server" CssClass="form-control" TextMode="MultiLine"></asp:TextBox></td>
                        </tr>
                        <tr>
                            <th>Condition: </th>
                            <td colspan="3">
```

<asp:TextBox ID="txtcomplaindesc" runat="server" CssClass="form-control" TextMode="MultiLine"></asp:TextBox></td>

<th>Medication: </th>

<td colspan="3">

<asp:TextBox ID="txtHdescription" runat="server" CssClass="form-control" TextMode="MultiLine"></asp:TextBox></td>

<th></th>

<td></td>

</tr>

<tr>

<th>Date:</th>

<td>

<asp:TextBox ID="dtDate" CssClass="form-control" runat="server" Width="350px"></asp:TextBox>

<script>

$j('#Main1_dtDate').Zebra_DatePicker({

// remember that the way you write down dates

// depends on the value of the "format" property!

//direction: [1, false],

//disabled_dates: ['* * * 0,6']

});</script> </td>

<th></th>

<td></td>

<td></td> <td>

<asp:Button ID="btnSubmit" class="btn btn-primary pull-right" runat="server" Text="Next" OnClick="btnSubmit_Click" /></td>

</tr>

</tbody>

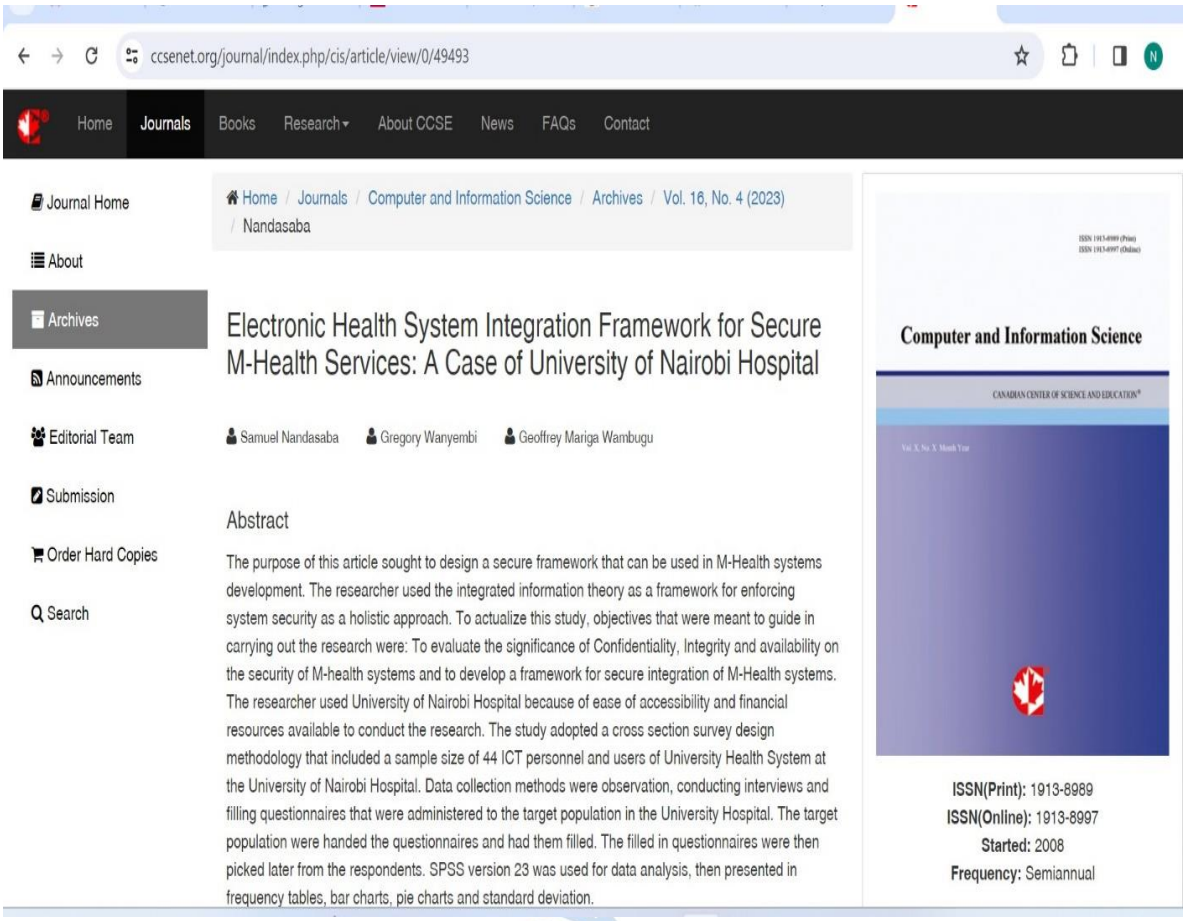
</table>

</asp:View>

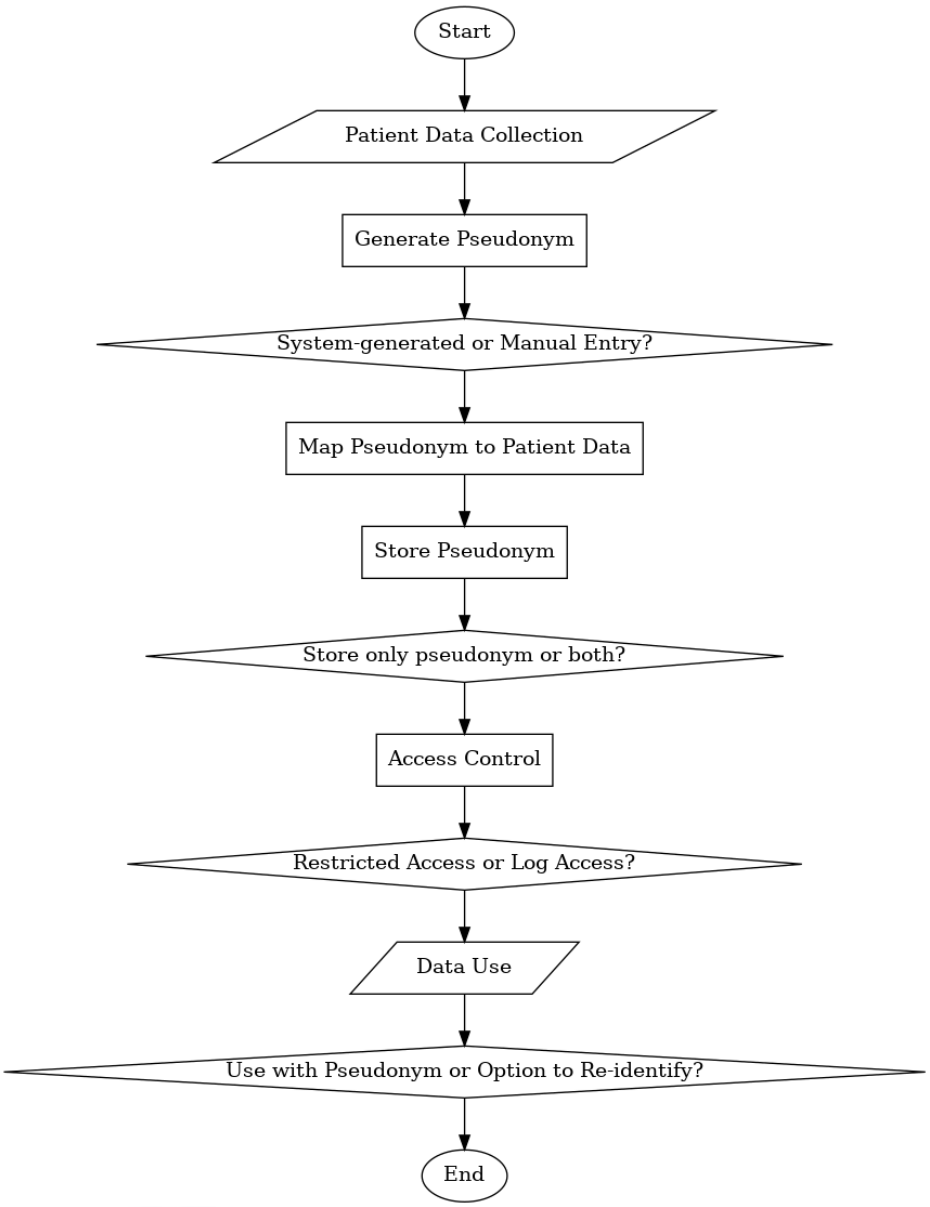
</asp:MultiView>

</section>

ix. Publication



x. Pseudonym Flow Chart


Start
Patient Data Collection
Generate Pseudonym
System-generated or Manual Entry?
Map Pseudonym to Patient Data
Store Pseudonym
Store only pseudonym or both?
Access Control
Restricted Access or Log Access?
Data Use
Use with Pseudonym or Option to Re-identify?
End