

**HEALTHCARE WORKERS' KNOWLEDGE OF PATIENT HEALTH DATA
PROTECTION WHEN USING DIGITAL HEALTH SOLUTIONS AT HOIMA
REGIONAL REFERRAL HOSPITAL**

JACQUELINE AINABYOONA

J24M21/007

**A DISSERTATION SUBMITTED TO THE FACULTY OF PUBLIC HEALTH, NURSING AND
MIDWIFERY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF
A DEGREE OF MASTER OF PUBLIC HEALTH OF UGANDA CHRISTIAN UNIVERSITY**

February, 2026



**UGANDA CHRISTIAN
UNIVERSITY**

A Centre of Excellence in the Heart of Africa

ABSTRACT

This study assessed healthcare workers' knowledge of patient health data protection when using digital health solutions at Hoima Regional Referral Hospital. As healthcare systems rapidly adopt the digital technologies, safeguarding the digital patient health data is vital for preserving trust and complying with the legal and ethical standards. However, inadequate knowledge of data protection principles among the healthcare workers using digital systems may compromise the security and privacy of patient health records. The study aimed to identify the digital health solutions used, assess healthcare workers' knowledge of patient health data protection principles and describe the data protection practices implemented within the hospital by the healthcare workers. A mixed methods approach was applied using structured questionnaires to collect data about the digital health solutions currently used, the knowledge of patient health data protection principles among the health care workers and their patient health data protection practices. The Interview guide was used to collect the patient health data protection practices among the healthcare workers in their respective departments. A sample of healthcare workers between the age of 31-50, most of whom were nurses, with the highest education qualification being between Diploma and Degree participated in this study. The findings revealed that UgandaEMR (E-Afya) was the most commonly used system (70.3%), followed by HMIS/DHIS2 (23.4%), Automated Laboratory Information Systems (3.9%) and Electronic Health Records (2.3%). The overall knowledge score on patient health data protection principles was moderate (54.7%). The most commonly reported patient data protection measure was the use of passwords or login credentials (74.2%). The findings showed that although digital health systems were widely used at Hoima Regional Referral Hospital, healthcare workers did not demonstrate strong knowledge of patient health data protection and had very low awareness of the Data Protection and Privacy Act (2019). The moderate knowledge level of the patient health data protection principles showed that some staff may not fully understand how to safeguard the sensitive patient information. In addition, relying mainly on passwords as a protection measure may leave the patient health data defenseless. Daily data protection practices were influenced by convenience, limited training and technical challenges which led to inconsistent patient data protection. These findings emphasized the need for more practical training and stronger institutional guidance to improve the secure management of patient health data.

DECLARATION

I hereby declare that this dissertation is my original work, not plagiarised and has not been submitted to any other institution for any award.

Signature:  Date: 19th/02/2026

Jacqueline Ainabyoona

Researcher

APPROVAL

This is to approve that the content in this report was done by Jacqueline Ainabyoona under the complete supervision and guidance from the university supervisor.

Supervisor's name: Dr. Edward Kibikyo Mukooza

Signature: 

Date: 19th/02/2026

DEDICATION

I humbly dedicate this dissertation to the Almighty God, the source of wisdom and understanding, who granted me the strength, resilience and grace to complete this work. May this achievement bring glory to Him. I further dedicate this work to my research supervisor who has been more than a supervisor but a mentor, to my loved ones, whose support and encouragement made this journey possible.

ACKNOWLEDGEMENT

I am greatly thankful to the Almighty God for being with me in every step of my academics. I as well extend my gratitude to Uganda Christian University that has given me a platform to express my skills through this learning journey.

I also thank my research mentor and supervisor, Dr. Edward Kibikyo Mukooza, whose multiple insights and guidelines issued, kept me on the right path and helped me to complete my research report.

Lastly, I thank the faculty of public health, nursing and midwifery for the addition of this valuable requirement to the program which has enriched me with the real-life applications of the knowledge with which I'm imparted during the program study at Uganda Christian University in my Master of Public Health.

TABLE OF CONTENTS

ABSTRACT	i
DECLARATION	ii
APPROVAL	iii
DEDICATION	iv
ACKNOWLEDGEMENT	v
LIST OF FIGURES	xi
LIST OF APPENDICES	xii
ACRONYMS & ABBREVIATIONS	xiii
OPERATIONAL DEFINITIONS OF TERMS	xiv
CHAPTER ONE	16
INTRODUCTION.....	16
1.1 Introduction	16
1.2 Background	17
1.2.1 Historical Background.....	17
1.2.2 Theoretical perspective.....	19
1.2.3 Conceptual perspective.....	19
1.2.4 Contextual perspective	20
1.3 Problem Statement	21
1.4 General objective.....	22
1.4.1 Objectives	22
1.5 Research questions	22
1.6 Study Scope.....	23
1.6.1 Content.....	23
1.6.2 Geographical.....	23
1.6.3 Time.....	23
1.7 Significance of the study	23
1.8 Conceptual Framework	24
CHAPTER TWO	26
LITERATURE REVIEW	26
2.1 Introduction	26
2.2 Theoretical review	26
2.3 Empirical Literature	28
2.4 Summary	35

CHAPTER THREE	38
METHODOLOGY	38
3.1 Introduction	38
3.2 Study Design	38
3.3 Population of the Study	39
3.4 Sample size determination	39
3.5 Sampling Techniques	40
3.6 Data Collection Methods.....	41
3.7 Data collection instruments.....	41
3.8 Data quality control.....	42
3.9 Data collection procedure.....	42
3.10 Data analysis	43
3.11 Ethical Considerations.....	43
CHAPTER FOUR.....	45
DATA ANALYSIS, PRESENTATION AND INTERPRETATION OF RESULTS.....	45
4.1 Introduction	45
4.2 Demographic Characteristics of Participants	45
4.3 Digital Health Solutions Used by the healthcare workers at Hoima Regional Referral Hospital	47
4.3.1 Types of Digital Health Tools and Frequency of Use	48
4.3.2 Analysis of the Number of Healthcare workers using each digital health solutions by Cadre.....	49
4.3.3 Analysis of Technical Confidence Levels	49
4.3.4 Bivariate Analysis showing Training Status vs. Confidence Level	50
4.3.5 Corelation between Age and Technical confidence when Using Digital Health Tools	51
4.4 Knowledge of Patient health data Protection Principles	51
4.4.1 Awareness of the Uganda Data Protection and Privacy Act (2019).....	52
4.4.2 Levels of Knowledge among Healthcare Workers (n=128).....	52
4.4.3 Correlation between Knowledge score, Education level and Usage Technical Confidence.....	53
4.4.4 Relationship between demographic variables, knowledge and usage confidence	54
4.4.5 Comparison of Knowledge across Data Protection Principles	55
4.4.6 The Education-Knowledge Gap	57
4.5 Patient health data Protection Practices	57
4.5.1 Primary Methods of Protecting Patient health data	58

4.5.2 Frequency of Patient health data Protection Behaviours.....	58
4.5.3 Application of Technical and Organizational Principles.....	59
4.5.4 Consistency of Protocol Adherence and Departmental Compliance.....	60
4.5.5 Primary Challenges to Effective Data Protection.....	61
4.5.6 Multiple Linear Regression Analysis of Digital Health Usage and Knowledge of Principles on Patient health data Protection Practices.....	62
4.6 Qualitative Analysis of Data Protection Practices	64
4.6.1 Access Control and the convenience vs security Experience.....	64
4.6.2 Technical Awareness and Encryption Gaps	65
4.6.3 Data Sharing, Consent and Assumed Consent	65
4.6.4 System Reliability and Departmental Silos	66
4.7 The Triangulation Matrix	67
CHAPTER FIVE	69
DISCUSSION OF FINDINGS	69
5.1 Introduction	69
5.2 Summary of findings.....	69
5.3 Demographics.....	69
5.4 Discussion of the findings concerning digital health solutions used by healthcare workers at HRRH.....	70
5.5 Discussion of the findings on Knowledge of Patient health data Protection Principles among healthcare workers at HRRH.....	72
5.6 Discussion of the findings on patient health data Protection Practices among healthcare workers at HRRH.	75
5.7 Study Limitations	78
CHAPTER SIX	79
CONCLUSIONS AND RECOMMENDATIONS.....	79
6.1 Introduction	79
6.2 Conclusion.....	79
6.2.1 Digital Health Solutions Used at HRRH	79
6.2.2 Knowledge of Patient health data Protection Principles	79
6.2.3 Patient health data Protection Practices.....	79
6.3 Recommendations	80
REFERENCES.....	82
APPENDICES	90
APPENDIX 1	90

APPENDIX 2 102

APPENDIX 3 105

APPENDIX 4 106

APPENDIX 5 106

APPENDIX 6 108

APPENDIX 7 111

LIST OF TABLES

Table 1: Sample size	40
Table 2: Descriptive results on characteristics of respondents	46
Table 3: Distribution of Staff Confidence Levels (n=128).....	50
Table 4: Association Between Age and Technical Confidence Using Spearman's Rank Correlation and Chi-Square Test.	51
Table 5: Levels of Knowledge among Healthcare Workers (n=128).....	53
Table 6: Spearman's Rank Correlation Between Knowledge Score, Education Level, and Usage Confidence	54
Table 7: Relationship Between Demographic Variables, Knowledge and Usage Confidence	54
Table 8: Perceived Importance of Confidentiality in Digital Health (n=128)	56
Table 9: Comparison of Academic Qualification and Practice Compliance (n=128)	57
Table 10: Primary Methods Used by Healthcare Workers to Protect Patient health data (n=128)	58
Table 11: Protocol Adherence and Departmental Compliance Ratings (n=128)	61
Table 12: Multiple Linear Regression Analysis of Digital Health Usage and Knowledge of Principles on Patient health data Protection Practices	62
Table 13: Triangulation of Quantitative and Qualitative Results (n=128)	67

LIST OF FIGURES

Figure 1: Usage of the digital health solutions at HRRH	48
Figure 2: Number of Healthcare workers using each digital health solutions by Cadre	49
Figure 3: Bivariate Analysis showing Training Status vs. Confidence Level	50
Figure 4: Awareness of the Data Protection and Privacy Act (2019) among the Healthcare staff	52
Figure 5: Staff understanding of specific data protection principles	56
Figure 6: Frequency of Data Protection Actions Among Staff (n=128).....	59
Figure 7: Application of Data Protection Principles (n=128).....	60
Figure 8: Primary Challenges to Effective Data Protection (N=128).....	62

LIST OF APPENDICES

APPENDIX 1	90
APPENDIX 2	102
APPENDIX 3	105
APPENDIX 4	106
APPENDIX 5	106
APPENDIX 6	108
APPENDIX 7	111

ACRONYMS & ABBREVIATIONS

HRRH	Hoima Regional Referral Hospital
WHO	World Health Organization
HMIS	Health Management Information System
DHIS2	District Health Information Software2
EMR	Electronic Medical Record
EHR	Electronic Health Record
EHRIS	Electronic Health Record System
EHMS	Electronic Health Management System
ICT	Information and Communication Technology
E-afya	Electronic Afya (Electronic Health)
ALIS	Automated Laboratory Information System
IV	Independent Variable
DV	Dependent variable
DOI	Diffusion of Innovation
TAM	Technology Acceptance Model
UTAUT	Unified Theory of Acceptance and Use of Technology
KAP	Knowledge, Attitudes, and Practices
PMT	Protection Motivation Theory
IT	Information Technology
ICU	Intensive Care Unit
OPD	Outpatient Department

OPERATIONAL DEFINITIONS OF TERMS

Digital Health Solutions: These refer to a broad range of electronic tools and systems used to improve health and healthcare delivery (World Health Organization, 2021). For this dissertation, Digital Health Solutions were defined as any electronic tools, software or systems used by healthcare workers at Hoima Regional Referral Hospital to collect, store, transmit or analyse patient health information. These solutions include, but are not limited to, the hospital's Electronic Health Record systems, District Health Information System 2 (DHIS2), telemedicine platforms and other mobile applications used for clinical tasks. This variable was measured by having healthcare workers self-report their use of specific systems, identifying the name of the solution, its primary function and how frequently it was used (Weik et al., 2024).

Healthcare Workers: These are professionals directly involved in the provision of health services (WHO, 2021). In this study, Healthcare workers were defined as all professional staff employed at Hoima Regional Referral Hospital who have direct clinical responsibilities and they included doctors, nurses, clinical officers and records officers. The sample was identified and selected from the hospital's official staff department registers of healthcare workers.

Knowledge of Patient health data Protection Principles

This refers to healthcare workers' cognitive understanding of the fundamental principles governing the protection of patient health information when using digital health solutions. The patient health data protection principles were confidentiality, integrity, availability, accountability, informed consent, access control as shown in the Uganda Data Protection and Privacy Act, 2019 and also in the Data Protection and Privacy Regulations, 2021. The researcher measured the healthcare workers' knowledge of patient health data protection principles using a questionnaire which assessed awareness of the legal requirements, the security rules and the ethical behaviours related to patient health data protection. Here, the scores were determined by the number of correct responses to the multiple-choice questions and the short answer questions in the questionnaire where a higher score indicated a high level of knowledge of patient health data protection principles, a medium score indicated moderate knowledge and a low score indicated limited or no knowledge of the principles.

Patient health data Protection Practices: These are specific actions and behaviours healthcare workers perform to ensure the confidentiality, integrity and availability of patient health data (Turkstani et., al 2025) when using digital health solutions. These practices are crucial for complying with legal requirements, like Uganda’s Data Protection and Privacy Act, 2019 which explicitly classifies health information as sensitive data and mandates stringent protection as it mandates data collectors, processors and controllers to adopt appropriate measures to secure the integrity of personal data in their control and maintaining patient trust.

The operational definition for this study was based on a combination of self-reported data from the questionnaires and interviews. The researcher measured the frequency and consistency of using strong, unique passwords and not sharing login credentials for access control, logging out of digital health systems after each session to prevent unauthorized access, adhering to the need-to-know principle, meaning workers only accessed the data necessary for their specific clinical tasks, proper handling and secure disposal of electronic devices like phones, tablets, computers that contain patient health data and using secure, hospital approved channels for transmitting patient health data, avoiding unencrypted platforms like personal email or messaging apps.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

This chapter looked at the background to the study, problem statement, purpose of the study, specific objectives, research questions, scope, significance and justification of the study.

The increasing adoption of digital health solutions has transformed healthcare service delivery by integrating technology to improve patient care, enhance efficiency and expand access to medical services. Digital health solutions include a variety of electronic health services some of which are those which are focused on the patient treatment support, those that simplify the management of the diseases and help healthcare workers to make decisions, those that improve managing of supply chain, health financing and those that help in collecting patient health data, using it and as well sharing it (Govender et al., 2022). Embracing digital health solutions, raises a serious concern of patient health data protection of which this protection to be offered, it needs the healthcare workers to have knowledge of the patient health data protection principles and apply these principles so as to safeguard the patient information and so making sure that healthcare workers are knowledgeable about patient health data protection principles and practices is essential for the healthcare facilities that use digital health solutions. Mudogo et al. (2023) show that whereas the digital health solutions improve access to healthcare services through remote service delivery, they also introduce patient health data privacy risks and insecurities.

This study, focused on Hoima Regional Referral Hospital located in Hoima City, Uganda, a major healthcare facility which is servicing at least seven districts in the Bunyoro region of western Uganda, with an estimated population of 2,300,000 people as shown by Mukobi et al. (2018). This referral hospital presented an ideal location from where the researcher assessed the healthcare workers' knowledge of patient health data protection principles when using digital health solutions. The findings from this research gave great understanding of the effectiveness, of the digital health solutions that were adopted in this hospital and the competence of the data protection practices among the healthcare workers.

1.2 Background

Background information was categorized into: historical, theoretical, conceptual and contextual perspectives.

1.2.1 Historical Background

According to Chief Healthcare Executive (2023), data breaches in the healthcare sector have escalated significantly, over the course of 2022, 71% of all health data breaches occurred in healthcare providers with over 50 million American patient records reportedly compromised which led to attacks like ransomware and hacking incidents. Insufficient cybersecurity practices and other major breaches have highlighted vulnerabilities in healthcare data systems and such breaches expose sensitive patient health data, including medical histories and financial details, underscoring the critical need for robust data protection measures in healthcare. A study conducted in Asia Pacific showed that nurses should be educated and trained in order to play a crucial role in promoting a culture of privacy and security as they often communicate patient information electronically through various channels such as email, messaging platforms and telehealth applications without using secure and encrypted communication methods to protect patient privacy (Nasrabadi et al., 2024) as it is because of their lack of patient health data protection knowledge that patient health data is accessed by unauthorised persons.

A cybersecurity knowledge and practice study conducted among nurses in South Africa showed that less than half, correctly understood basic terminology about cyber related issues like strong passwords, antivirus, information passed as part of a typical web page request, ransomware and phishing and the majority understood the purpose of encryption (79.3%). More than half of participants (67.4%) understood what spam was, but less than half (42.4%) understood all the characteristics of strong passwords. On the other hand, confidentiality, consent and data security were often overlooked and they required further guidelines for general utilisation, legal compliance, device (personal and hospital) utilisation and data transfer (encryption) of health information (Singh et al., 2022) hence their poor implementation of patient health data protection measures.

In Uganda, the healthcare system is progressively adopting digital health solutions, such as the District Health Information System (DHIS2) and other electronic platforms for managing patient

health data. Despite these advancements, unauthorized access to patient information has raised significant concerns about compliance with data protection principles and practices and this unauthorised access is not only external but also internal among these very health care workers. A survey conducted in 15 districts, with 180 respondents distributed across 8 Electronic Health Information System initiatives showed that 85% of the respondents evaluated their Electronic Health Information System but only 25% had standard guidelines in form of clear-cut methods or mechanisms to conduct the evaluation (Nagwovuma et al., 2021) which means that different healthcare providers are following different rules that as well govern patient health data protection.

Uganda has been embracing Digital health technologies like Telemedicine, Electronic Medical Records Systems, social media campaigns among others so as to improve healthcare service delivery however, implementation of these technologies has not been easy because of some issues like inadequate funding, computer illiteracy and lack of healthcare infrastructure. Developed countries like Canada have rising health care support and funding by their governments (Fisk et al., 2020) which is not the case in some developing countries as just healthcare service delivery is accompanied by trials such as inadequate funding and weak healthcare infrastructure (NANKUNDA et al., 2020).

At Hoima Regional Referral Hospital, the utilisation of Digital Health solutions for all healthcare workers started in October, 2024 where every healthcare worker was given a digital tool, and so the use of digital tools such as electronic health records to store patient health records is growing significantly hence the research. However, there was a pressing need to assess the extent of healthcare workers' knowledge of data protection principles when using these digital health solutions as preliminary observations suggest potential risks to patient confidentiality due to unintentional or mishandling of sensitive information. While various studies have addressed that healthcare workers lack knowledge of digital patient health data protection principles and have suggested training programs for health workers, introduction of digital security rules, several loopholes persist like clearly understanding and researching on how these healthcare workers use these digital health solutions and what they use them for so as to get clear insight on why their knowledge could be low concerning the use of these digital health solutions for patient health data protection as reasons could in-tail the specific tools used and what they are used for, how

this hospital complies to the specific legal regulations, the available technological resources not only focusing on training them to use tools that they may not eventually employ at work. Plus, the rapid pace of technological innovation often outpaces the capacity of healthcare workers to stay updated on best practices for data protection and so given these underlying loopholes, this study focused on healthcare workers' knowledge of patient health data protection principles when using digital health solutions at Hoima Regional Referral Hospital aiming at assessing how well healthcare workers protect patient health data when using digital health solutions while adhering to data protection principles, identifying knowledge gaps and providing recommendations to enhance the security of patient health data when using digital health solutions.

1.2.2 Theoretical perspective

This study adopted Protection Motivation Theory (PMT), developed by Rogers (1975) and the Knowledge, Attitudes and Practices (KAP) model. The PMT explains how knowledge and perception of a risk, motivates individual to adopt protective behaviour showing how healthcare workers could implement data security mechanisms because there is a certain possibility of a threat like a data breach, un authorized access to patient health data manipulating a weakness in the digital health solutions, and so PMT stresses that the motivation of protection gets to increase when there is a threat (Floyd et al., 2000). PMT points out the very importance of knowledge such that healthcare workers can apply patient health data protection principles effectively. The KAP model complements PMT by offering a practical framework that is to be used to assess the health care workers' knowledge of the patient health data protection principles and practices thus allowing the researcher to measure what the healthcare workers knew, and what they actually did as they used these digital health solutions at Hoima Regional Referral Hospital.

Therefore, these two models together provided a robust framework for understanding and addressing gaps in knowledge, motivation and practices related to patient health data protection among healthcare workers at Hoima Regional Referral Hospital.

1.2.3 Conceptual perspective

Patient health data protection in tails measures and practices that ensure the confidentiality, integrity and security of personal health information in the healthcare and this data encompasses

personal information, medical records, treatment plans and diagnostic results (Nasrabadi et al., 2024). Healthcare workers have to protect patient confidentiality under laws or regulations (Determann et al., 2019). Digital Health Utilisation is the use of communication technology to address gaps in the health sector (Mudogo et al., 2023). Digital health interventions are health services conveyed electronically and are categorized into four groups; interventions for clients by offering health promotion materials and treatment support, interventions of healthcare providers including disease management information, decision making support, interventions for a health system offering supply chain management, health financing and data services interventions for data management, usage and its sharing (Govender et al., 2022). These digital health solutions have become essential to modern healthcare systems by providing tools that improve disease awareness, enhance treatment and restructure patient care. However, implementing of patient health data protection while using these technologies mainly depends on the knowledge healthcare workers have concerning the protection of patient health data as healthcare professionals need to understand how to protect sensitive patient health data and ensure compliance with patient health data protection laws and regulations.

1.2.4 Contextual perspective

Hoima Regional Referral Hospital incorporated digital health solutions like electronic health records, Electronic Medical Record systems into their patient data handling. Despite the fact that the digital health solutions are being used, observations and reports showed that many healthcare workers lacked adequate knowledge on how to secure patient health data when using these digital solutions (Namatovu et al., 2021) and also on data privacy regulations like the Uganda's 2019 Data Protection and Privacy Act, leaving weighty gaps in compliance and risk mitigation. Furthermore, audits of digital health system usage showed gaps in securing patient information, raising concerns about potential data breaches and violations of confidentiality on patient health data. This gap in knowledge compromises patient trust and as well undermines the effectiveness of digital health technologies in enhancing healthcare delivery, requiring urgent interventions to address this critical issue as patients could feel the no need to use them. However, there were almost no existing observed studies that were conducted to address the issue of patient health data protection knowledge among healthcare workers generally among hospitals in Uganda that

use digital health solutions which empowered this study with the aim of assessing the knowledge of the patient health data protection principles and practices of healthcare workers regarding data protection, with the goal of promoting the secure use of digital health solutions.

1.3 Problem Statement

The use of digital health solutions has changed healthcare delivery by enhancing efficiency, improving patient care and streamlining the health service provision. However, the privacy of digital patient health data depends on the healthcare workers' knowledge of patient health data protection when using the digital health solutions as patient health data protection is a very important pillar of digital healthcare which ensures that the sensitive health information is kept confidential and secure. Weak data security practices can lead to data breaches, unauthorized access and privacy violations, which compromise patient confidentiality, expose institutions to legal and financial risks, and undermine trust in digital healthcare services. Moore et al. (2019) showed that data breaches do happen regularly than it seems and that the existing legal and technical safeguards are insufficient.

Although there is some use of digital health solutions at Hoima Regional Referral Hospital, healthcare workers may not have satisfactory knowledge of the patient health data protection principles when using the digital health solutions which may lead to insufficient patient health data protection practices. This difference may compromise the patient health data privacy thus exposing the sensitive information to unauthorized users. The problem is not that they don't have a legal framework to follow because the Uganda's Data Protection and Privacy Act of 2019 clearly classifies patient health information as sensitive and requires the healthcare workers who handle and use this data to implement data integrity measures. However, studies show that Uganda continues to face challenges related to awareness and technological capacity that may lead to improper handling of patient health data (Moore et al., 2019) and yet concerns about data security risks may slow down the acceptance of the digital health solutions which may in the end limit the potential benefits of these solutions improving healthcare delivery (Nasrabadi et al., 2024).

There is limited research on how well healthcare workers at Hoima Regional Referral Hospital understand and apply patient health data protection principles when using the digital health

solutions at the facility even if the Uganda National eHealth Strategy emphasized the need for evaluating the usage of digital health solutions among the healthcare workers and so addressing this gap is crucial to strengthen patient health data security and build up confidence in the digital healthcare systems.

The findings identified knowledge gaps, inform training and policy recommendations and enhanced secure digital health adoption to safeguard patient health data and improve healthcare outcomes.

1.4 General objective

To examine the healthcare workers' knowledge of Patient Health Data Protection when using digital health solutions at Hoima Regional Referral Hospital.

1.4.1 Objectives

1. To identify the digital health solutions used by healthcare workers at Hoima Regional Referral Hospital.
2. To assess the knowledge of patient health data protection principles among healthcare workers in Hoima Regional Referral Hospital using digital health solutions.
3. To describe the patient health data protection practices of healthcare workers in the use of digital health solutions.

1.5 Research questions

1. What digital health solutions are used by healthcare workers at Hoima Regional Referral Hospital, and how do they describe their purpose and frequency of use?
2. What is the level of knowledge that healthcare workers at Hoima Regional Referral Hospital have about patient health data protection principles when using digital health solutions?

3. What patient health data protection practices are implemented by healthcare workers when using digital health solutions, and what are their experiences in maintaining these practices?

1.6 Study Scope

This research focused under three different scope as undermentioned.

1.6.1 Content

The study was limited to examining the healthcare workers' knowledge of patient health data protection principles and practices when using digital health solutions at regional referral hospitals using a case study of Hoima Regional Referral Hospital. This aimed to investigate the extent to which healthcare workers understood and applied data protection principles on patient health data when using digital health tools to measure how well digital health solutions were working and how patient health data therein was secure at the hospital, if the staff were knowledgeable and followed proper data protection practices.

1.6.2 Geographical

The research was conducted at Hoima Regional Referral Hospital which is located in Hoima city, situated opposite Booma grounds which are along Hoima, Kampala-road.

1.6.3 Time

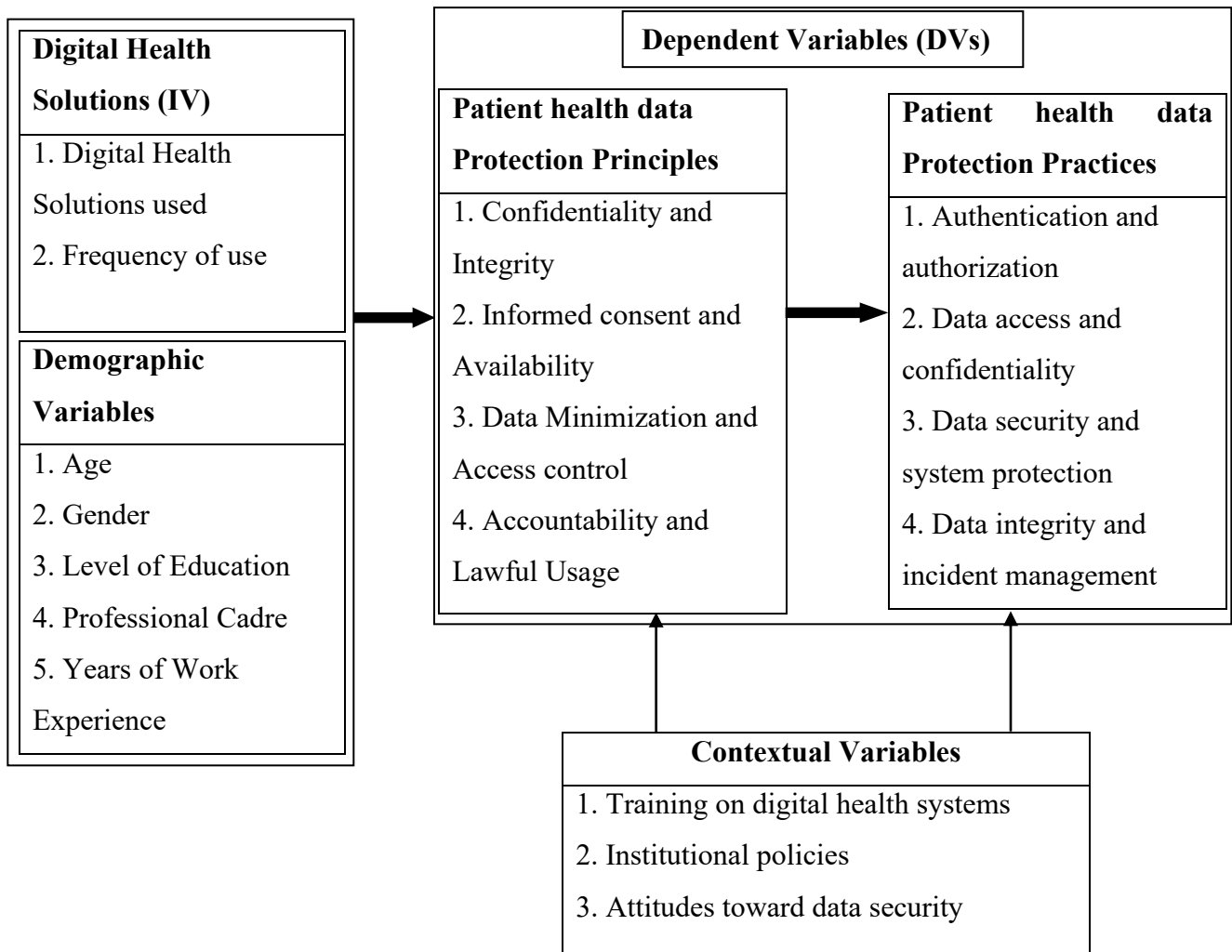
The researcher collected data in a period between November-December 2025, and the data collected was relevant for that time of data collection.

1.7 Significance of the study

Successful implementation of health information technology innovations has numerous benefits to healthcare providers, physicians, patients and society. Increasingly, securing digitized health data is becoming an unstated mandate when developing and deploying these innovations (Parthasarathy et al., 2021). The study addressed healthcare workers' knowledge of patient health data protection principles when using digital health solutions by examining the healthcare workers' knowledge, experiences and the practices they carried out when using digital health solutions. This study thus gave understanding that can guide the training of healthcare workers, improve compliance with the data protection rules, address the available serious gaps in digital

patient health data security (Sittig et al., 2016) and also contribute to designing and adhering to stronger policies and regulations, such that the healthcare workers have the knowledge on how to mitigate data breach risks and so protect the privacy of the patients (Bărcanescu, 2021).

1.8 Conceptual Framework on healthcare workers' knowledge of Patient Health Data Protection when using Digital Health Solutions at Hoima Regional Referral Hospital



This study's conceptual framework shows how the use of digital health solutions influences healthcare workers' knowledge of patient health data protection principles and their data protection practices at Hoima Regional Referral Hospital.

The independent variable is the use of digital health solutions and it includes systems like EHR, HMIS and DHIS2. It also covers how they are used, such as for data entry, reporting and diagnosis, how often they are used and the departments where they are used like OPD, maternity, and laboratory.

The dependent variable has two parts. The first is knowledge of patient health data protection principles. This includes understanding confidentiality, integrity, informed consent, data access control and lawful use of data. The second is data protection practices, which include password use, access control, device security and handling of data breaches.

The framework also includes demographic factors like age, gender, education level, job role and work experience as these may affect both knowledge and practices.

There are also contextual factors such as training, institutional policies and attitudes toward data security, which can influence how digital health systems affect knowledge and practices.

This framework assumes that using digital health systems more effectively improves knowledge and leads to better data protection practices among healthcare workers.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This literature review offered a summary of existing research on the digital health solutions used by healthcare workers, their knowledge of patient health data protection principles and the practices they carried out to protect patient health data. This gave an understanding of the theoretical and practical basis for addressing the gaps in the healthcare workers' knowledge of the principles and practices concerning patient health data protection as they used the digital health solutions in their health facilities. Therefore, through detailed analysis and evaluation of the related studies, this chapter gave the differences and their contributions to this study.

2.2 Theoretical review

Some scholars have studied how healthcare workers understand patient health data protection when using digital health tools. The Technology Acceptance Model (TAM) by Davis (1989) proposes that people use technology, based on how easy it is to use and how useful it seems which in other words explains why healthcare workers choose to use tools like electronic health records or telemedicine (Masrom et al., 2007).

TAM is widely used in healthcare to study the utilization of technology among the healthcare workers, but it does not focus on patient health data protection knowledge. It mainly looks at usefulness and ease of use of technology, but not the risks of data breaches or security issues, which are important for this study.

In addition is the Diffusion of Innovations Theory (DOI) developed by Everett Rogers (1962). DOI theory explores how innovations spread within a social system as it emphasizes that new ideas, technologies or practices are adopted through a process involving knowledge, persuasion, decision, implementation and confirmation (García-Avilés et al., 2020). Much as the Diffusion of Innovations theory could explain how digital health solutions were adopted by healthcare workers making it relevant for understanding how healthcare workers made use of digital health solutions and how these solutions were used to store patient health data for example, healthcare workers perceived digital health solutions as having significant advantages over traditional methods. It was not directly focused on data protection knowledge as it was more concerned with

the overall adoption of innovations rather than the motivations to protect patient health data once the technology was adopted since it assumes that once a technology is adopted, it is used effectively to simply store data.

Furthermore, the Unified Theory of Acceptance and Use of Technology (UTAUT) developed by Venkatesh et al. (2003) which combines elements from eight different models of technology acceptance proposes four key factors that determine technology acceptance and these are performance expectancy, effort expectancy, social influence and facilitating conditions and these affect both the intention and actual use of technology (Williams et al., 2015). The UTAUT model gave a simple way to understand how healthcare workers accept the using of digital health solutions, social influence and the conditions provided at work, like the training and organizational support, play an important role in whether users of digital solutions who were the healthcare workers in this research used these tools correctly, especially for protecting patient information. UTAUT integrates a wide range of factors that influence technology adoption, making it particularly useful for understanding the complex organizational context of healthcare settings and also considers social influences, which are crucial in healthcare environments where peer behaviour and leadership affect data protection practices. Although UTAUT addresses technology adoption and use, it does not focus directly on motivational aspects related to data protection for example how individuals feel about protecting patient health data or whether they feel capable of doing so and it does not capture the specific security concerns or the psychological mechanisms behind adopting data protection measures, which are central to this study.

This study identified Protection Motivation Theory (PMT) which asserts that individuals are motivated to protect themselves and sensitive data from threats when they perceive these threats as severe, likely to occur and are within their ability to prevent or manage which integrates two key components that is threat appraisal which involves evaluating the severity of a potential threat like data breaches and the likelihood of hacking of health data and coping appraisal where health workers assess their ability to take protective actions for example implementing security measures on the patient health data.

In addition to PMT, the Knowledge, Attitudes, and Practices (KAP) model, originally developed in public health research for assessing behavioural outcomes, was relevant to this study. The model suggests that a person's knowledge influences their attitudes, which in turn affect their practices (Launiala, 2009; WHO, 2008). In the healthcare context, it allows researchers to determine whether healthcare workers' understanding of patient health data protection principles translates into actual protective behaviours when using digital health solutions.

The Diffusion of Innovations (DOI) theory, Technology Acceptance Model (TAM), and UTAUT model all helped clarify how digital health solutions were made use of by the healthcare workers, but none of these models focused on whether healthcare workers had knowledge on how to protect patient health data and as well how they behave when handling it, when using the digital health solutions. In contrast, the KAP model allowed for the assessment of knowledge and practices, while Protection Motivation Theory (PMT) explained the motivations behind protective behaviours by considering threat perception, self-efficacy and response efficacy. KAP and PMT offered a framework for understanding both what the healthcare workers knew and did, and why they acted towards the protect patient health data which made them much more applicable for this study.

2.3 Empirical Literature

Digital health solutions used by healthcare workers

Kavuta and Magoiga (2023) assessed the usability of a health information system at Geita Regional Referral Hospital in Tanzania and found it to be widely accepted by healthcare workers due to its user-friendly features, such as ease of navigation, data retrieval and support for routine clinical tasks. While the study confirmed the active use of a digital health tool in a referral hospital, it did not specify the type or name of the system, leaving a gap in identifying which specific digital health solutions were in use an area this study sought to address at Hoima Regional Referral Hospital.

Mwogosi and Mambile (2025) conducted a survey study to examine the adoption and utilisation of electronic health record systems (EHRS) in Tanzanian public primary healthcare facilities and the usage of these platforms were 62.3% for GoTHoMIS, 17.2% for eHMS and 6.6% for Care2X of which these low percentages stressed that training among the healthcare workers, interoperability and data security influence system adoption. However, the study focused exclusively on electronic health record systems and did not examine other digital health technologies such as telemedicine, mobile health apps, electronic logistics systems or laboratory information systems. This presented a knowledge gap, as it limited understanding of the full range of digital health solutions currently used by healthcare workers particularly in higher level facilities like Hoima Regional Referral Hospital, where a broader variety of technologies may be deployed to support service delivery.

Babughirana et al. (n.d.) conducted a feasibility assessment of scaling up electronic-supported solutions to improve maternal, newborn and child health interventions in Hoima District, with a focus on identifying and evaluating digital health tools such as CommCare, mHealth and the District Health Information System 2 (DHIS2). The study examined infrastructure and network readiness at sub-county and health facility levels, including mobile network coverage. Findings showed that while digital systems like DHIS2 and HMIS had been deployed in the district, only 44.2% of the staff had received training on DHIS2 and just 37.2% had access to HMIS and could transmit reports through it. The availability of powered, internet-enabled computers and modems was limited, with only 20.9% of facilities reporting access. Additionally, 55.8% of facilities had staff trained in basic computer skills, though only 46.5% were proficient, and 54% of sampled staff could carry out basic digital operations such as using a mouse and keyboard. This study provided direct evidence of the digital health systems in use in Hoima and highlights both the potential for scale-up and the current limitations in access, infrastructure and workforce readiness.

While Babughirana et al. identified digital health solutions used in Hoima District like the CommCare, DHIS2, mHealth and assessed infrastructure and staff training at health facility level, the study did not specifically focus on Hoima Regional Referral Hospital hence the need to

identify the digital health solutions used by healthcare workers at Hoima Regional Referral Hospital.

Tumuhimbise et al. (2023) carried out a research on acceptability and feasibility of a mobile health application for enhancing public private mix for TB care among healthcare workers in Southwestern Uganda where three private hospitals and a public hospital in southwestern Uganda received the Tuuka mobile application and this was used for referring patients by healthcare workers from private hospitals and receiving referred patients by public healthcare workers and sending SMS reminders to the referred patients. Tuuka application was accepted by healthcare workers with a mean total system usability scale score of 98 (SD 1.97). The majority believed that the app would help them make quicker medical decisions (91%), communicate with other healthcare workers (96%), facilitate partnerships with other hospitals (100%), and enhance quick TB case notification (96%). The application was perceived to be useful in reminding referred patients to adhere to referral appointments, notifying public hospital healthcare workers about the incoming referred patients, facilitating communication across facilities, and enhancing patient-based care. The study found out that the mobile health solutions can make communication and coordination in healthcare easier but, it did not look closely at whether or not healthcare workers knew how to use the Tuuka app well and how they even kept the patient health data secure while using this Tuuka app and because of this, there was still limited understanding of how the patient health data was protected on these digital health solutions.

Bostan et al. (2024) explained that open-source Electronic Health Record (EHR) systems can help improve healthcare in low and middle-income countries by making it easier to collect, manage and analyze data. Systems like OpenEMR were free to use and can be changed to fit the needs of local health facilities. These systems helped healthcare workers save and access patient information more easily. However, the study did not mention how the healthcare workers use free digital health solutions in their daily work. Also, this study pointed out major security problems, like the risk of SQL injection and unauthorized access, but did not explain how these systems were protected against such attacks when being used by the healthcare workers, a gap which showed the need for the current study, to find out which digital health tools were used at

Hoima Regional Referral Hospital and how their digital health solutions were being secured so as to safeguard the patient health data on them.

Healthcare workers' knowledge of patient health data protection principles when using digital health solutions

Healthcare workers' understanding of patient health data protection principles is very important for keeping digital health information private, accurate and secure. Khatiwada et al. (2024) stated that even if electronic patient health data is now widely used, many healthcare workers still have in adequate knowledge about data security, privacy and accuracy in digital systems. While some measures, like restricting access to data and applications, were used to prevent unauthorized access, these methods were often applied without proper training or understanding, which showed the need for healthcare workers to be well-trained in managing access to protect patient information. Nevertheless, this study did not measure knowledge among the healthcare workers and how it differed among the different healthcare workers who are doctors, nurses, records officers and this was important gap for focusing training and support to the healthcare workers who use the digital health tools.

Alunyu et al. (2024) emphasized that healthcare workers need both proper digital health communication systems and training so as to have the knowledge on how to use them effectively. Even if 83.3% of respondents said that some basic skills are needed to use these systems safely, the study did not show how much healthcare workers actually knew about protecting patient health data, how they applied these data protection principles when using the digital health solutions. Also, there was little evidence on whether or not the training programs really helped healthcare workers to handle patient health data securely, which was the focus of the current study, at Hoima Regional Referral Hospital.

Takuwa et al. (2023) studied about the using of mobile health solutions in Uganda and found that healthcare and veterinary workers had many concerns about keeping data private, controlling access, and maintaining security. Some workers knew about the risks, a small number of 3% had never used mHealth, showing a knowledge difference of both using the digital health solutions

and as well properly securing the health data there on. The study also showed the low electronic health literacy, limited training and weak infrastructure among the healthcare workers, which make it harder for them to use digital health systems efficiently, but, it did not show how much healthcare workers actually knew about key patient health data protection principles, like keeping information confidential, controlling access, and handling data securely.

Kwesigabo and Komba (2025) also studied how healthcare workers in Tanzania handle cybersecurity, and they found out that the healthcare workers' knowledge of patient health data protection was only moderate, with an average score of 3.07 out of 5 stressing it that normal training was limited, scoring just 2.39 on average and many workers felt that protecting data was not part of their role, frequently leaving it to the ICT officers. This study on the other hand did not show differences in knowledge among specific staff groups who regularly managed patient health data when using the digital health solutions.

Mensah et al. (2024) found out that healthcare workers do generally understand the basic patient health data protection principles, like privacy, confidentiality, secure access and the need for administrative safeguards but, there are no measurements that actually show the scores of the healthcare workers to prove the percentage of them that know and to also know the percentage of the group that did not know.

Patient health data protection practices of healthcare workers in the use of digital health solutions

Yeng, Fauzi, and Yang (2022) studied how healthcare workers followed cybersecurity rules in hospitals that do not use paper records but rather, use digital health solutions mainly focusing on the practices like managing passwords, using email and social media safely, securing mobile devices and reporting problems based on hospital policies meant to prevent data breaches. Using the Knowledge, Attitude, Behavior framework, the study found that the healthcare workers generally knew what to do as the knowledge risk was low, with the mean of 1.59, but their actions did not always match this knowledge since the behavior risk was high, mean of 2.72. This shows that even if policies exist, healthcare workers may not always follow them in practice.

However, this study was done in hospitals with better equipment and support than most of the public hospitals in Uganda like Hoima Regional Referral Hospital which adopted the using of digital health solutions for all their healthcare workers in October 2024, thus the need to carry out this research, so as to find out the practices the healthcare workers at Hoima Regional Referral Hospital are implementing when handling patient health data while using the digital health solutions.

Gebeyew et al. (2025) studied how healthcare workers in the Amhara Region of Ethiopia handled digital health data and they found out that more than half which was about 55% had poor data protection practices, while only 45% followed good practices. In a referral setting hospital, the average score was 5.19, with 28% of men and 17% of women handling the health data securely. Even though the digital solutions were being widely used, healthcare workers often did not manage patient health data safely whereby one person said, “we download everything, the expert is not as knowledgeable as to handle system security problems,” and another said, “we do not use data encryption because we do not have enough skills.”

These comments showed that these healthcare workers did not even know how to implement the patient health data protection practices and even did not know the principles they should adhere to as there were gaps in knowing about encryption, system security and proper ways to handle patient health data. Also, some healthcare workers relied only on simple passwords for they did not understand that encryption was important, which showed limited awareness of digital health security and so the study stressed the need to improve both knowledge and safe practices among healthcare workers.

Bagyendera, Nabende, and Nabukenya (2023) studied the main factors affecting data use and system interoperability in Uganda’s healthcare system, looking at four regions: Central, West Nile, South-Western and Northern. They found out that sharing information among healthcare facilities was being weakened by the lack of standard operating procedures and the poor documentation for accessing and handling electronic medical records and that without clear procedures, healthcare workers do not have proper guidance on how to handle patient health data safely.

The study also found out that 36% of respondents said, there were no effective data security policies, which made it harder to create secure ways of handling the patient health data in the digital health solutions. Complying to security principles was inadequate and many health ICT systems work in separation without ongoing support which forced healthcare workers to use informal and sometimes unsafe methods to manage the patient health data. In addition, many healthcare workers lacked technical skills and training, which created another barrier to protecting the patient health data handled on these digital health solutions. This study showed the need for this research, to describe the patient health data protection practices implemented by healthcare workers because it did not show them.

Kwesigabo and Komba (2025) studied how healthcare workers handled patient health data when using the digital health solutions where they found many unsafe habits, like sharing passwords with colleagues with a score of 95%, using weak passwords with a score of 76%, and reusing the same login across systems with a score of 31%. The study also showed more security problems like forged documents which went up from two cases in 2023 to four in 2024, and unauthorized disclosures of the patient health data increased from one to three. The study also looked at the implementation of data integrity by the healthcare workers and the score was 3.18 out of 5 which is moderate, confidentiality where they scored 2.67 which is low to moderate, and availability of patient health data with a score of 4.24 which was very high, meaning that healthcare workers focus on seeing to it that patient health data is available in the digital health solutions but, they did not pay enough attention to keeping it safe and private of which these weak practices put sensitive patient information at risk.

Kayondo and Kyobe (2025) studied about what affects healthcare workers' following Uganda's Data Protection and Privacy Act and they found out that having a good workplace culture, regular training, clear rules, make it easier for healthcare workers to protect patient health data when using the digital health solutions. This study also showed that 62% of workers had 6 to 10 years of experience handling patient health data, while 38% had less than five years, meaning that workers with more experience feel more confident and are more likely to follow the rules as they are experienced and they also said in their study that training can help workers feel confident and handle data safely.

This study did not explain exactly what healthcare workers do to protect the patient health data for example, it did not state that the healthcare workers use passwords, control who can see data, or share data safely when using digital tools which was an important gap that the current study looked at, what healthcare workers at Hoima Regional Referral Hospital actually did to protect patient health data when using digital health solutions.

Ogbodo et al. (2025) studied what affects healthcare workers' compliance to data protection rules and they found out that good hospital management had a very strong effect on how well the healthcare workers followed the rules, with a score of 0.832. Encrypting patient health data, controlling access and checking for threats, also had a big effect, with a score of 0.739 and that over 70% of healthcare workers used their own devices for work, which led to problems like data leaks or unauthorized access of patient health data.

The study showed that less experienced workers depend more on hospital rules to protect data, while more experienced workers follow better cybersecurity practices because they knew the systems and have been using them longer which shows that both healthcare worker habits and hospital rules are important to keep patient health data safe.

2.4 Summary

The reviewed literature provided an overview of the usage of digital health solutions, healthcare workers' knowledge of the patient health data protection principles and the patient health data protection practices.

Digital Health Solutions Used by Healthcare Workers

The reviewed literature showed that digital health solutions were being adopted and used in various healthcare settings. Studies from Tanzania showed that electronic health record (EHR) systems like GoTHoMIS, eHMS were widely used because they had user-friendly features, which streamline clinical tasks and data retrieval (Kavuta & Magoiga, 2023; Mwogosi & Mambile, 2025). Similarly, research in Uganda confirmed the positive use of mobile health applications for patient referrals for TB care (Tumuhimbise et al., 2023).

Despite these findings, gaps remained in understanding how practically these tools are being used by healthcare workers although they confirmed that they had digital tools, they often fell

short of detailing how frequently they used them, for what specific clinical purposes and the healthcare workers' technical confidence in their use (Mwogosi & Mambile, 2025). The work of Babughirana et al. (n.d.) identified specific systems like DHIS2 and CommCare used in the Hoima District and also showed that a significant percentage of staff lacked basic computer skills and training on how to use the systems.

Although the digital health solutions were being used, there was limited evidence on the specific roles for which the healthcare workers used them and how frequently they used them in clinical practice. Understanding the actual digital health solutions in use and what kind of data were used there on was important to support effective data protection measures.

Healthcare Workers' Knowledge of Patient health data Protection Principles

Many healthcare workers using digital health systems did not fully understand how to protect patient data though they could have been using basic protection measures like limiting access using passwords they still lacked proper training to do it correctly. It is not clear how knowledge differs between doctors, nurses, clinical officers and records staff, even though all handle patient information. Some of the healthcare workers leave the responsibility to ICT staff, showing confusion about their roles and yet they know basic ideas like integrity and confidentiality. They often do not understand technical protections and also their understanding of data protection principles under Uganda's Data Protection and Privacy Act, 2019 is not shown, making it necessary for further research to be done.

Patient health data Protection Practices

The literature reviewed shows that many healthcare workers did not follow proper patient data protection practices, even if they knew the principles. Studies from Referral hospitals using digital health solutions found unsafe behaviours like sharing passwords, storing user account logins on the computer and not encrypting data. In Uganda, lack of knowledge of the practices, the policies present that are to be followed and low technical skills made staff rely on informal and insecure ways to manage data. How healthcare workers handle data on a daily like making use of authentication, access controls, secure patient health data sharing and on whether practices

differ between systems like EHRs and EMRs and so showing the need for more research to see how workers actually protect patient data in daily practice and where improvements are needed.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter consists of the research methodology used to assess the healthcare workers' knowledge of patient health data protection when using digital health solutions at Hoima Regional Referral Hospital covering the Study Design, Population, Sample size, Sample size determination, Sampling techniques, Data collection methods, Data collection instruments, Data quality control, Data collection procedure, Data analysis and Ethical Consideration.

3.2 Study Design

The study made use of a mixed-methods design with both quantitative and qualitative approaches to provide an understanding of the research problem. The quantitative section used a non-experimental, cross-sectional design. This approach was effective for gathering broad, statistical data from a sample of healthcare workers at a single point in time, providing a clear snapshot of the level of knowledge of patient health data protection principles and the patient health data protection practices. This design was highly effective for identifying the digital solutions and assessing knowledge of patient health data protection principles.

The qualitative section used a descriptive case study design using specifically Hoima Regional Referral Hospital as the case which was particularly appropriate to the third research objective, as it allowed for an in-depth exploration of the how and what questions behind healthcare workers' patient health data protection practices (Yin, 2018). By using interviews, there was illumination of the contextual factors, challenges and motivations that could not be fully captured through a survey alone. These designs provided a strong framework for the study, first quantifying the extent of the issue and then enriching those findings with a rich, contextual understanding of the factors at play (Creswell & Creswell, 2018).

3.3 Population of the Study

The population of this study was comprised of healthcare workers at Hoima Regional Referral Hospital who were using of digital health solutions, as well as responsible for patient health data protection and they were the doctors, nurses, records officers, laboratory technicians, dentists, midwives and clinical officers. The population was chosen to understand the digital health solutions they use, their knowledge of patient health data protection principles and the patient health data protection practices they do to see to it that the digital patient health data is secure. Also, the research aimed to gather understanding into the challenges they face, effectiveness of their practices in healthcare delivery.

3.4 Sample size determination

The study used both quantitative and qualitative approaches where by the sample size for the quantitative component was determined using Cochran's formula for an infinite population, which was then adjusted for the actual population of healthcare workers involved in digital health solution use at Hoima Regional Referral Hospital (N = 192).

Cochran's formula for an infinite population;

$$n_0 = \frac{Z^2 \cdot p \cdot (1-p)}{e^2}$$

Z=1.96 (Z-score for 95% confidence level)

p=0.5 (estimated proportion for maximum variability)

e=0.05 (margin of error)

$$n_0 = \frac{(1.96)^2 \cdot 0.5 \cdot (1 - 0.5)}{(0.05)^2} = \frac{3.8416 \cdot 0.25}{0.0025} = 384.16$$

$$n = \frac{n_0}{1 + \frac{n_0 - 1}{N}} = \frac{384}{1 + \frac{383}{192}} = \frac{384}{3} = 128$$

Therefore, the total sample size was 128 participants. For the qualitative section, the sample size of 14 participants was selected through purposive sampling as they were chosen based on their specialized knowledge, roles within the hospital and firsthand experience related to patient health

data protection practices. According to Crossman (2018), purposive sampling is used to identify key informants who can provide rich, relevant and focused information to deepen understanding of the research study. The researcher personally approached these healthcare workers to invite their participation and explained the purpose of the study.

Table 1: Sample size

Healthcare workers	Target population	Sample Size
Doctors	23	15
Nurses	82	54
Midwives	43	29
Dentists	6	4
Lab Technicians	13	9
Records Officers	4	3
Clinical Officers	21	14
Total	192	128

$$\text{Cadre Sample Size} = \frac{\text{Target population}}{\text{Finite Population (192)}} \times (\text{Total Sample Size})128$$

3.5 Sampling Techniques

The researcher used stratified random sampling for the quantitative research approach of this study such that each subgroup within the healthcare workers at Hoima Regional Referral Hospital was represented. This method provided more precise estimates and comprehensive insights into the healthcare workers' knowledge of patient health data protection when using digital health solutions across different professional groups which were doctors, nurses, records officers, laboratory technicians, dentists, midwives and clinical officers. The researcher divided the healthcare workers into different strata based on their roles and departments and then she randomly selected a proportional sample from each subgroup making sure that the sample reflected the actual distribution of the healthcare workers within the hospital.

And for the qualitative approach, the researcher used purposive sampling technique, strategically selecting healthcare workers at Hoima Regional Referral Hospital who possessed specific characteristics or experiences relevant to the third research objective as this method was ideal for

gathering in-depth insights from participants who had direct experience with patient health data protection practices when using digital health solutions. The participants included records officers because they directly handle patient records and can provide insights on data protection practices, doctors because they enter and use patient health data in digital health systems, nurses because they interact with patient health data during care and documentation, midwives because they record the number maternal cases handled, lab technicians because they record and store the various laboratory checkups done on patients and clinical officers because they may use digital health tools for diagnostics and treatment data, as these individuals are directly involved in managing, accessing and even using patient health data in digital health systems.

3.6 Data Collection Methods

This study used a questionnaire survey to collect data from doctors, nurses, records officers, midwives, laboratory technicians and clinical officers who were using the digital health solutions about the digital health solutions they use and their knowledge of patient health data protection principles. A questionnaire is a structured set of questions prepared to obtain information from respondents in a systematic way (Gulnoza et al., 2022). Also, both closed ended and open-ended questions were used to receive authentic and subjective responses making the data complete and easy to analyse. In addition, interviewing method was also used and here, the researcher gathered information through direct verbal interaction with the healthcare workers who use the digital health solutions to identify the patient health data protection practices.

3.7 Data collection instruments

This study employed two primary data collection instruments that was a self-administered questionnaire and an interview guide with each instrument tailored to the respective categories of respondents and their contents were designed to gather the necessary data to address the research objectives. The researcher used a self-administered questionnaire to collect data from all the selected healthcare workers involved in the use of digital health solutions at Hoima Regional Referral Hospital. The questionnaire included both closed-ended questions using Likert scale measurement and open-ended questions, which allowed respondents to provide both quantitative data so as to capture respondents' knowledge and understanding of patient health data protection

principles as well as their experiences and challenges in implementing the patient health data protection when using digital health solutions. The instrument was structured to ensure clarity and ease of completion, allowing respondents to express their views while ensuring data uniformity for analysis. In addition, an interview guide was used to collect in-depth qualitative data from key personnel including doctors, nurses, records officers, midwives, laboratory technicians, dentists and clinical officers responsible for digital patient health data maintenance to describe their patient health data protection practices. The interview guide consisted of open-ended questions that were structured to elicit more specific and in-depth responses related to organizational practices, challenges and strategies for implementing digital health solutions and data protection measures.

3.8 Data quality control

To ensure the quality of the data collected, both validity and reliability of the instruments was rigorously addressed where validity was ensured through expert review of the questionnaire and interview guide for content accuracy, pilot testing to assess clarity and relevance and alignment with the research objectives. Reliability was tested using test-retest reliability to check consistency over time, internal consistency through Cronbach's alpha for the questionnaire and inter-rater reliability for interviews by comparing multiple interviewers' analyses.

3.9 Data collection procedure

The researcher obtained permission to conduct research and collect data by first securing clearance from Uganda Christian University Research Ethics Committee and then received an introductory letter from Uganda Christian University which she used to approach Hoima Regional Referral Hospital to formally request permission and guidance on data collection procedures of which after being granted permission, the researcher coordinated with respondents to schedule sessions for data collection. The researcher utilized a combination of structured and semi-structured questionnaires, featuring both multiple-choice and open-ended questions, as well as interviews with the respective participants. The data collection process was systematic, ensuring that tools were appropriately distributed and responses were gathered effectively and after data collection, the researcher proceeded and did data processing and analysis and also ensured ethical standards like obtaining informed consent plus maintaining respondent confidentiality, throughout the process.

During data collection, some selected healthcare workers declined to participate in the study. However, these were replaced with other eligible participants from the same study population until the required sample size of 128 was achieved. All the final 128 participants who were approached completed the study.

3.10 Data analysis

The collected data was first edited and cleaned to ensure completeness, consistency and accuracy. The data then be categorized based on participants' responses from both questionnaires and interviews.

For the quantitative data, responses from the structured questionnaires were entered into Microsoft Excel and analysed using the python programming language. Descriptive statistics, including percentages was computed at the univariate level. Bivariate analysis, such as cross-tabulations, Spearman's coefficient correlation were conducted to examine relationships between variables, particularly between healthcare workers' characteristics like education, experience, technical confidence and their knowledge of patient health data protection principles.

This study also adopted an Explanatory Sequential Mixed Methods Design, where the quantitative phase was conducted first to assess healthcare workers' knowledge of patient health data protection principles. The results of the quantitative analysis were used to inform the qualitative phase, guiding the development and refinement of the interview guide. This approach allowed the researcher to explore in-depth the areas where knowledge gaps or patterns are identified.

For the qualitative data, interview responses were transcribed and analyzed using thematic and content analysis. Key themes and patterns was identified to gain a deeper understanding of participants' experiences, perspectives and practices related to patient health data protection.

3.11 Ethical Considerations

The researcher first received ethical clearance from the Uganda Christian University Research Ethics Committee and then approached Hoima Regional Referral Hospital to formally seek permission and guidance on collecting the data needed for the study. Informed consent was received from all the participants, seeing to it that they were fully informed about the study's objectives, their roles and their rights to confidentiality and anonymity. Ethical morals were as a

must followed to safeguard the participants' privacy. Sensitive data was handled with utmost security and all collected data, including survey responses and interview records were made unknown to prevent including any identifiable information in research documents. The data collected was stored in a secure manner with access restricted to only the researcher, participants' identities were protected in the final report and no personal information was disclosed.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND INTERPRETATION OF RESULTS

4.1 Introduction

This chapter presents the study results on healthcare workers' digital health solutions used, their knowledge of patient health data protection principles and their patient health data practices when using digital health solutions at Hoima Regional Referral Hospital. The results are based on the information which was got through structured questionnaires and the interviews following an Explanatory Sequential Mixed Methods Design.

Specifically, it presents the demographic characteristics of the respondents, presentation of both descriptive and inferential results in relation to identifying the digital health solutions currently in use, assessing the level of knowledge healthcare workers possess regarding patient health data protection principles and describing the data protection practices being applied when using the digital health solutions. The chapter also reveals how the quantitative results informed the qualitative phase to provide a deeper understanding of the experiences and challenges these health care workers faced in maintaining data privacy when using the digital health solutions.

4.2 Demographic Characteristics of Participants

The characteristics of the 128 respondents included in the study which were gender, age, department, job title, years of professional experience and level of education are presented. It is important to understand these background characteristics because they affect the knowledge levels of the patient health data protection principles and data protection practices of healthcare workers regarding patient health data at Hoima Regional Referral Hospital.

Table 2: Descriptive results on characteristics of respondents

Variable	Category	Frequency (n=128)	Percentage (%)
Gender	Male	50	39.1
	Female	78	60.9
Age Group	25-30	24	18.8
	31-40	47	36.7
	41-50	40	31.2
	51-60	17	13.3
Department	Outpatient Department	28	21.9
	Maternity	53	41.4
	Surgery	18	14.1
	Gynaecology	9	7.0
	ICU	5	3.9
	Medical ward	2	1.6
	Laboratory	9	7.0
	Dental Department	4	3.1
Job Title	Medical Doctor	15	11.7
	Nurse	54	42.2
	Record Officer	3	2.3
	Lab Technician	9	7.0
	Clinical Officer	14	10.9
	Midwives	29	22.7
	Dentist	4	3.1
Years of Experience	Less than 1 year	6	4.7
	1 to 3	18	14.1
	4 to 6	35	27.3
	More than 6	42	32.8
	Above 10	27	21.1
Education Level	Certificate	1	0.8

Variable	Category	Frequency (n=128)	Percentage (%)
	Diploma	76	59.4
	Bachelor's Degree	49	38.3
	Master's Degree	2	1.6

Table 2 shows the results of the demographic characteristics of the 128 respondents. Majority of respondents were female 60.9% (n = 78), while males constituted 39.1% (n = 50) with 31-40 years 36.7% (n = 47) and 41-50 years 31.2% (n = 40). Participants who were between 25-30 years had a score of 18.8% (n = 24), while those aged 51-60 years with a representation of 13.3% (n = 17).

The highest number of respondents came from the Maternity Department 41.4% (n = 53), followed by the Outpatient Department 21.9% (n = 28). The Surgery, Gynaecology, ICU, Laboratory, Dental and Medical Ward departments had smaller proportions.

The nurses job title formed the largest group 42.2% (n = 54), followed by Midwives 22.7% (n = 29), Medical Doctors 11.7% (n = 15), and Clinical Officers 10.9% (n = 14). Other cadres such as Laboratory Technicians, Dentists and Records Officers were less represented with less percentages.

About the years of professional experience, most respondents had more than six years of experience 32.8% (n = 42), followed by those with 4-6 years 27.3% (n = 35). Respondents with over ten years of experience constituted 21.1% (n = 27), while those with less than one year were the least at 4.7% (n = 6).

In terms of education level, the majority of respondents were Diploma holders 59.4% (n = 76), followed by those with a Bachelor's Degree 38.3% (n = 49) and very few respondents held a Certificate 0.8% (n = 1) or a Master's Degree 1.6% (n = 2).

4.3 Digital Health Solutions Used by the healthcare workers at Hoima Regional Referral Hospital

This section presents the results regarding the types of digital health tools adopted by healthcare workers, the frequency of their application in clinical and administrative tasks.

4.3.1 Types of Digital Health Tools and Frequency of Use

The study identified a variety range of digital tools utilized for clinical and administrative functions and the primary tools include Electronic Health Records, HMIS/DHIS2, UgandaEMR/E-Afya and Automated Laboratory Information Systems.

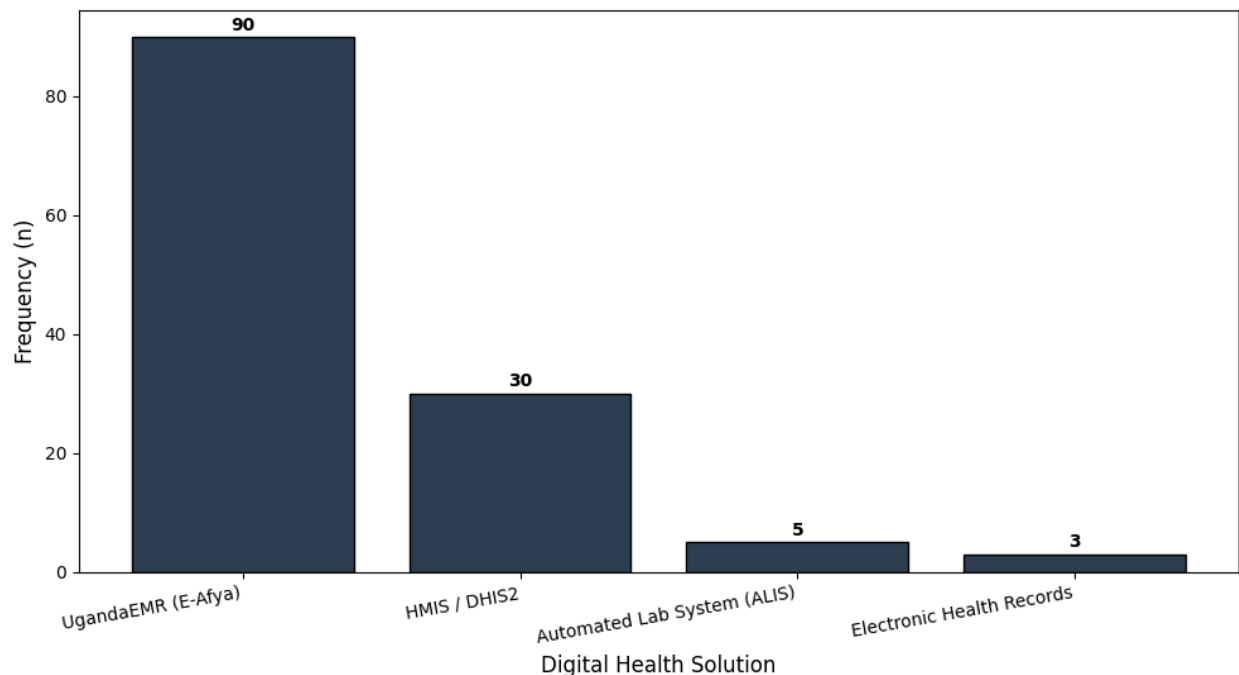


Figure 1: Usage of the digital health solutions at HRRH

The results in Figure 1 show that UgandaEMR (E-Afya) was the mostly used digital health solution with a high score of 70.3% (n = 90) of respondents. HMIS/DHIS2 was the second most utilized system with a score of 23.4% (n = 30) of the respondents. Automated Laboratory Information Systems were reported by 3.9% (n = 5) of respondents, while general Electronic Health Records were used by 2.3% (n = 3).

4.3.2 Analysis of the Number of Healthcare workers using each digital health solutions by Cadre

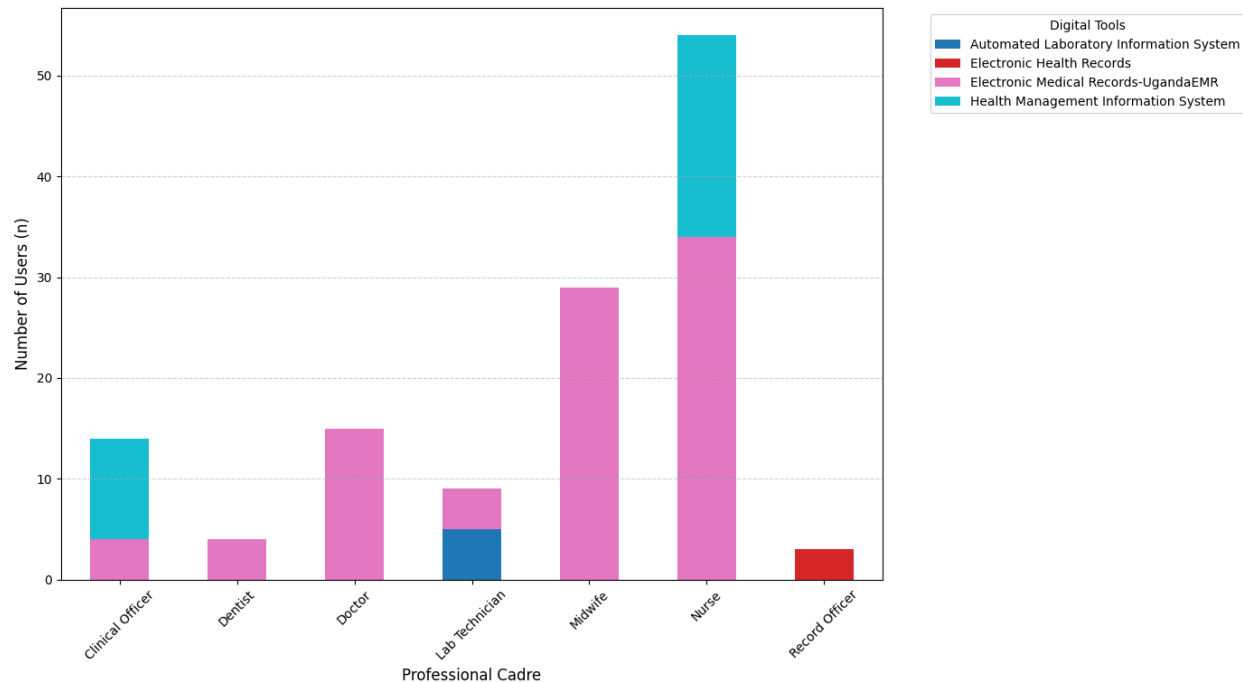


Figure 2: Number of Healthcare workers using each digital health solutions by Cadre

Figure 2 presents the distribution of digital health tool usage by professional cadre. The results show that UgandaEMR was used by 15 Doctors, 34 Nurses, 4 Clinical Officers, 29 Midwives, and 4 Dentists. Automated Laboratory Information Systems (ALIS) were used exclusively by 5 Laboratory technicians. Electronic Health Records were used by 3 Record Officers, Health Management Information Systems (HMIS) were used by 10 Clinical officers and 20 Nurses.

4.3.3 Analysis of Technical Confidence Levels

Before assessing legal knowledge, the study measured the self-reported confidence of healthcare workers in using digital health tools as confidence is a key indicator of user readiness.

Table 3: Distribution of Staff Confidence Levels (n=128)

Confidence Level	Frequency (n)	Percentage (%)
Very Confident	4	3.1%
Confident	88	68.8%
Somehow Confident	36	28.1%
Total	128	100.0%

The results in Table 3 show that 68.8% (n = 88) of respondents reported being confident in using digital health tools. A total of 28.1% (n = 36) indicated that they were somehow confident, while 3.1% (n = 4) reported being very confident.

4.3.4 Bivariate Analysis showing Training Status vs. Confidence Level

A bivariate analysis was conducted to examine the relationship between training status and self-reported confidence levels in the use of digital health tools.

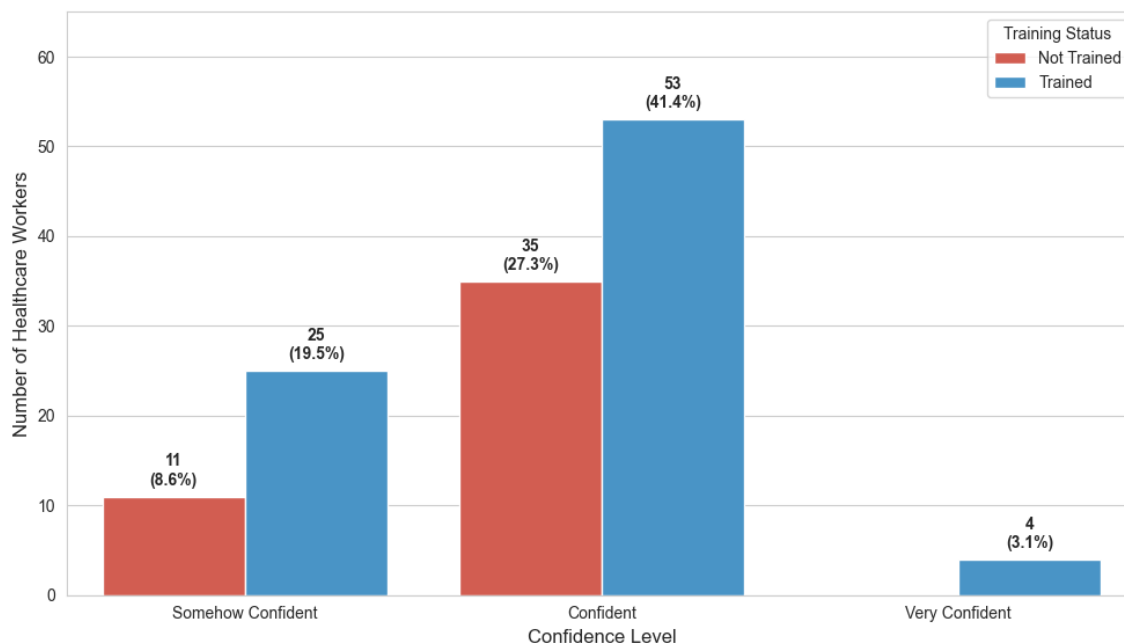


Figure 3: Bivariate Analysis showing Training Status vs. Confidence Level

The results in Figure 3 show that among trained staff (n = 82), 53 reported being confident, 25 were somehow confident, and 4 were very confident. Among staff who

had not received training (n = 46), 35 reported being confident, 11 were somehow confident and none reported being very confident.

4.3.5 Corelation between Age and Technical confidence when Using Digital Health Tools

To assess the relationship between age and technical confidence in the use of digital health tools, respondents were grouped by age and their reported confidence levels were analyzed.

Table 4: Association Between Age and Technical Confidence Using Spearman's Rank Correlation and Chi-Square Test.

Variables	Spearman's ρ	X ² (value)	df	p-value	Cramer's V	Strength
<i>Age vs. Technical Confidence</i>	-0.380	26.800	12	0.008*	0.264	Moderate

A moderate negative correlation was observed between age and technical confidence with Spearman's $\rho = -0.380$, $p = 0.008$, indicating that confidence tends to decrease with increasing age. The Chi-square test also indicated a significant association $\chi^2 = 26.800$, $df = 12$, $p = 0.008$, with a moderate strength of association as measured by Cramer's V 0.264.

4.4 Knowledge of Patient health data Protection Principles

The second objective of this study is to assess the level of knowledge that healthcare workers at Hoima Regional Referral Hospital have about patient health data protection principles. These principles include confidentiality, integrity, availability, accountability, informed consent, lawful usage, access control and data minimization, as outlined in the Data Protection and Privacy Act (2019). As defined in the operational terms, this knowledge refers to the staff's understanding of the rules that protect patient health information when using digital tools.

4.4.1 Awareness of the Uganda Data Protection and Privacy Act (2019)

The study assessed the level of awareness of the Uganda Data Protection and Privacy Act (2019) among healthcare workers and Figure 4 below shows the distribution of respondents based on their awareness of the Act.

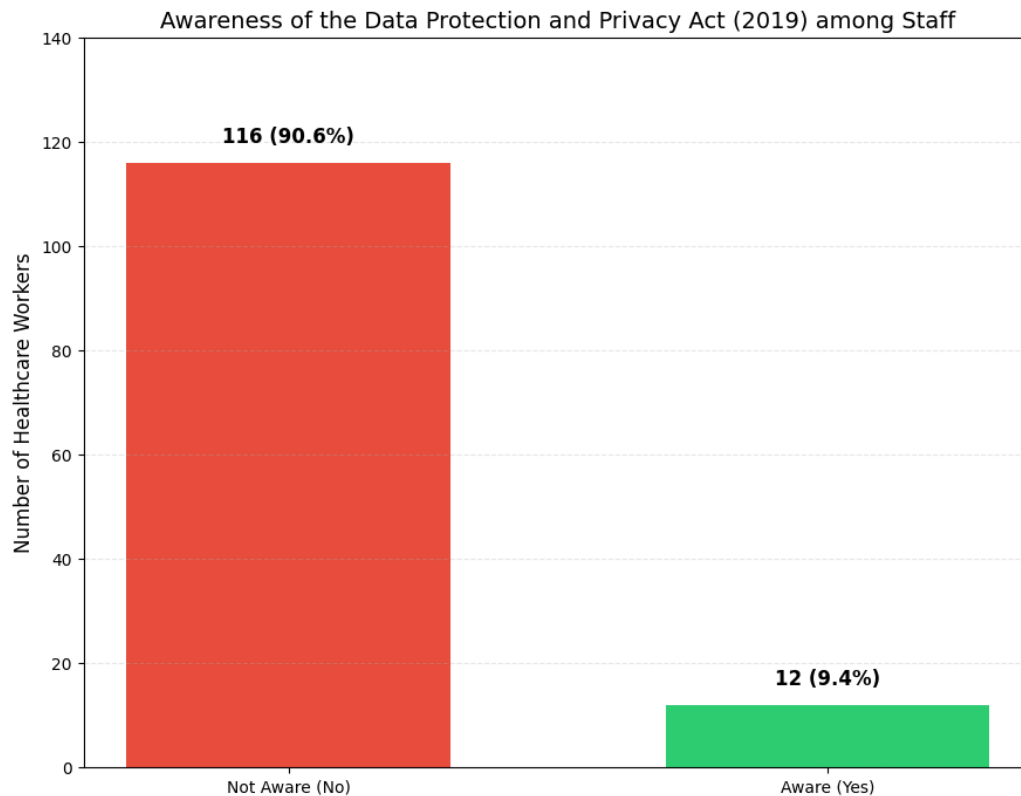


Figure 4: Awareness of the Data Protection and Privacy Act (2019) among the Healthcare staff

The results in Figure 4 show that 12 respondents (9.4%) were aware of the Uganda Data Protection and Privacy Act (2019) and 116 respondents (90.6%) were not aware of the Act.

4.4.2 Levels of Knowledge among Healthcare Workers (n=128)

To assess the level of knowledge among healthcare workers, a scoring range was used based on nine (9) items which derived from the questionnaire. Each respondent received one point for each item they reported being aware of or understanding which resulted in a maximum possible score of nine (9).

The items assessed included awareness of the Data Protection and Privacy Act (2019), confidentiality, data integrity, data availability, accountability, informed consent, lawful processing, access control and data minimization.

Respondents were categorized into three knowledge levels based on their total scores. Scores of 0-3 were classified as Low Knowledge, scores of 4-6 as Moderate Knowledge and scores of 7-9 as High Knowledge.

Table 5: Levels of Knowledge among Healthcare Workers (n=128)

Knowledge Level	Score Range	Frequency (n)	Percentage (%)
High Knowledge	7 - 9	43	33.6%
Moderate Knowledge	4 - 6	70	54.7%
Low Knowledge	0 - 3	15	11.7%
Total		128	100.0%

The results in Table 5 show that 54.7% (n = 70) of respondents were classified as having a Moderate level of knowledge. A total of 33.6% (n = 43) were classified as having High knowledge, while 11.7% (n = 15) were classified as having Low knowledge.

4.4.3 Correlation between Knowledge score, Education level and Usage Technical Confidence

Table 6 below shows the correlations between Knowledge Score, Education Level and Usage Technical Confidence. Knowledge Score was measured as a total of the Data Protection principles and Usage Confidence was measured based on staff technical confidence levels.

Table 6: Spearman's Rank Correlation Between Knowledge Score, Education Level, and Usage Confidence

Variables	Spearman's ρ	p-value	Strength
Knowledge Score vs. Usage Confidence	0.307	0.000*	Moderate
Education Level vs. Knowledge Score	0.140	0.114	Weak
Education Level vs. Usage Confidence	0.103	0.245	Weak

$p < 0.05$

Spearman's rank correlation analysis showed a moderate positive and statistically significant relationship between Knowledge Score and Usage Confidence ($\rho = 0.307$, $p < 0.001$).

No statistically significant relationship was observed between Education Level and Knowledge Score ($\rho = 0.140$, $p = 0.114$) or between Education Level and Usage Confidence ($\rho = 0.103$, $p = 0.245$).

4.4.4 Relationship between demographic variables, knowledge and usage confidence

Table 7: Relationship Between Demographic Variables, Knowledge and Usage Confidence

Demographic Variable	vs. Knowledge Score (ρ)	vs. Usage Confidence (ρ)	p-value (Knowledge)	p-value (Usage)
Age	-0.767	-0.380	0.000*	0.000*
Experience (years)	-0.668	-0.341	0.000*	0.000*
Gender	-0.005	-0.223	0.955	0.011*
Job Title	-0.238	-0.132	0.007*	0.139
Department	-0.082	-0.018	0.356	0.837

Spearman's rank correlation was used to examine the relationship between demographic variables, Knowledge Score and Usage Confidence. Age showed a strong negative correlation

with Knowledge Score ($\rho = -0.767$, $p < 0.001$) and a moderate negative correlation with Usage Confidence ($\rho = -0.380$, $p < 0.001$), indicating that increases in age were associated with lower knowledge and confidence levels.

Similarly, years of experience demonstrated a strong negative correlation with Knowledge Score ($\rho = -0.668$, $p < 0.001$) and a moderate negative correlation with Usage Confidence ($\rho = -0.341$, $p < 0.001$), suggesting that more experienced staff tended to report lower knowledge and confidence regarding digital health tools.

Gender showed almost no relationship with Knowledge Score ($\rho = -0.005$, $p = 0.955$), indicating no meaningful association. However, it exhibited a weak but statistically significant negative correlation with Usage Confidence ($\rho = -0.223$, $p = 0.011$), suggesting minor differences in confidence levels across gender.

Job title demonstrated a weak negative but statistically significant correlation with Knowledge Score ($\rho = -0.238$, $p = 0.007$), implying that variations in job roles were associated with differences in knowledge levels. However, its relationship with Usage Confidence was weak and not statistically significant ($\rho = -0.132$, $p = 0.139$), indicating that job title did not meaningfully influence confidence.

Department showed weak and non-significant correlations with both Knowledge Score ($\rho = -0.082$, $p = 0.356$) and Usage Confidence ($\rho = -0.018$, $p = 0.837$), suggesting that departmental affiliation did not have a measurable impact on either knowledge or confidence in this study.

4.4.5 Comparison of Knowledge across Data Protection Principles

The researcher analyzed staff understanding of the eight data protection principles. Figure 5 presents the proportion of staff demonstrating high knowledge for each principle.

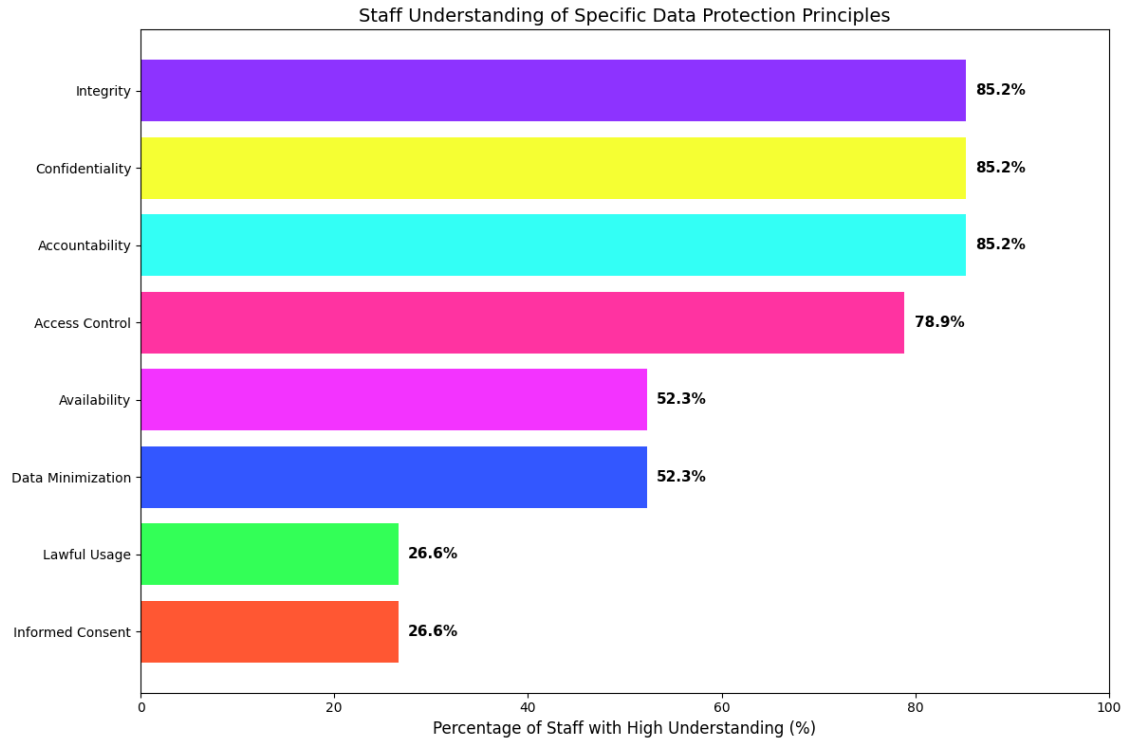


Figure 5: Staff understanding of specific data protection principles

The results in figure 5 indicate variation in knowledge across the principles. High understanding was observed in Confidentiality, Integrity and Accountability (85.2%), followed by Access Control (78.9%). Moderate understanding was found in Data Minimization and Availability (52.3%), while Informed Consent and Lawful Usage had the lowest high understanding at 26.6%.

Table 8: Perceived Importance of Confidentiality in Digital Health (n=128)

Importance Level	Frequency (n)	Percentage (%)
Very Important	118	92.2%
Important	10	7.8%
Not Important	0	0.0%
Total	128	100.0%

As shown in Table 8, out of 128 participants, 118 (92.2%) rated data confidentiality as very Important, while 10 (7.8%) rated it as important. No participant considered confidentiality as Not Important.

4.4.6 The Education-Knowledge Gap

The study identifies that while the workforce is educated, there is a significant difference between general academic attainment and specific knowledge of the Data Protection and Privacy Act (2019) principles, which indicates that institutional knowledge is not a natural byproduct of medical training.

Table 9: Comparison of Academic Qualification and Practice Compliance (n=128)

Qualification	Total Respondents	High Practice Compliance (n)	Compliance Rate (%)
Certificate	1	0	0.0%
Diploma	76	9	11.8%
Bachelor's Degree	49	7	14.3%
Master's Degree	2	0	0.0%
Total	128	16	12.5%

As shown in Table 9, out of 128 respondents, 16 (12.5%) demonstrated high compliance with data protection practices. Among diploma holders, 9 out of 76 (11.8%) showed high compliance. For respondents with a bachelor's degree, 7 out of 49 (14.3%) demonstrated high compliance. None of the respondents with certificate or master's qualifications recorded high compliance.

4.5 Patient health data Protection Practices

The results related to patient health data protection practices among healthcare workers at Hoima Regional Referral Hospital are presented here and these included the use of strong passwords and regular password changes, session security (logging out immediately after accessing patient health data) and the use of encryption measures.

4.5.1 Primary Methods of Protecting Patient health data

Table 10: Primary Methods Used by Healthcare Workers to Protect Patient health data (n=128)

Primary Protection Method	Frequency (n)	Percentage (%)
Use of passwords or login credentials	95	74.2%
Regularly logging out of the system after use	23	18.0%
Avoiding the sharing of login details	10	7.8%
Encrypting or restricting file access	0	0.0%
Total	128	100.0%

As shown in Table 10, the majority of respondents, 95 out of 128 (74.2%), reported using passwords or login credentials as their primary method of protecting patient health data. A total of 23 respondents (18.0%) indicated that regularly logging out of the system after use was their main practice. 10 respondents (7.8%) identified avoiding the sharing of login details as their primary protection method. None of the respondents reported using file encryption or technical access restrictions as their primary method of protecting patient health data.

4.5.2 Frequency of Patient health data Protection Behaviours

The frequency of the patient health data protection behaviours were analysed and respondents rated their behaviours on a scale ranging from Never to Always. The actions assessed included using strong passwords and changing them regularly, ensuring data accuracy, encrypting data, and logging out immediately after using digital health systems.

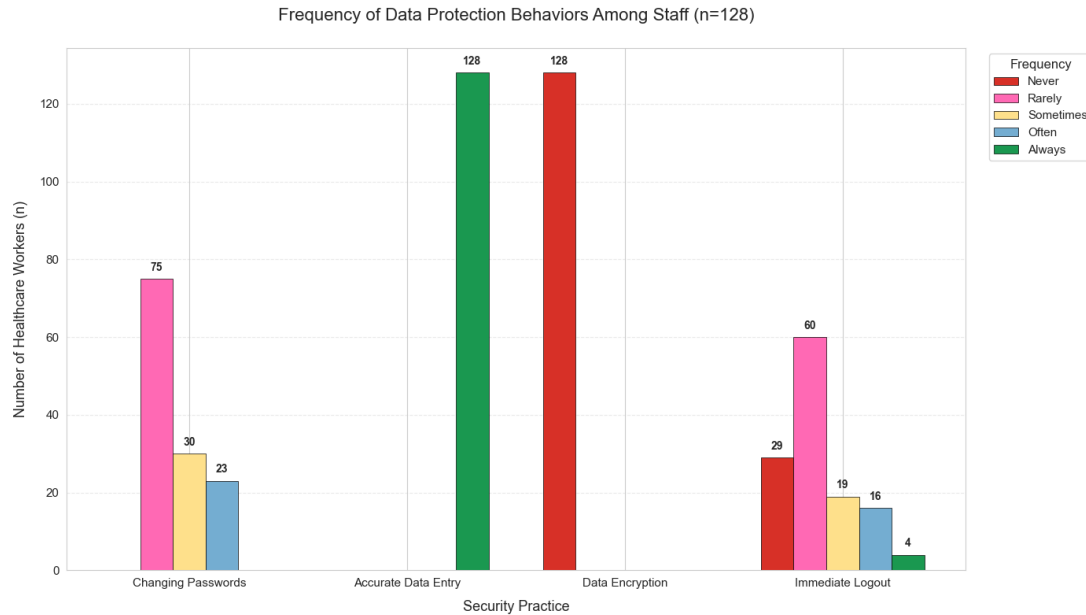


Figure 6: Frequency of Data Protection Actions Among Staff (n=128)

As shown in Figure 6, all respondents (100.0%) reported that they always ensure the accuracy of the data they enter. 75 respondents (58.6%) reported that they rarely use strong passwords and as well rarely change passwords regularly as 30 (23.4%) reported sometimes and 23 (18.0%) reported often. No respondents reported always change passwords regularly.

For logging out after use, 60 respondents (46.9%) reported that they rarely log out immediately after using the digital health solutions, while 29 (22.7%) reported never doing so. Only 4 respondents (3.1%) reported always logging out after completing their tasks.

With regard to encryption of data, all respondents (100.0%) reported that they never encrypt or lock digital files.

4.5.3 Application of Technical and Organizational Principles

The study assessed how healthcare workers at Hoima Regional Referral Hospital apply selected technical and organizational principles under the Data Protection and Privacy Act (2019) and the principles examined were Access Control and Data Minimization.

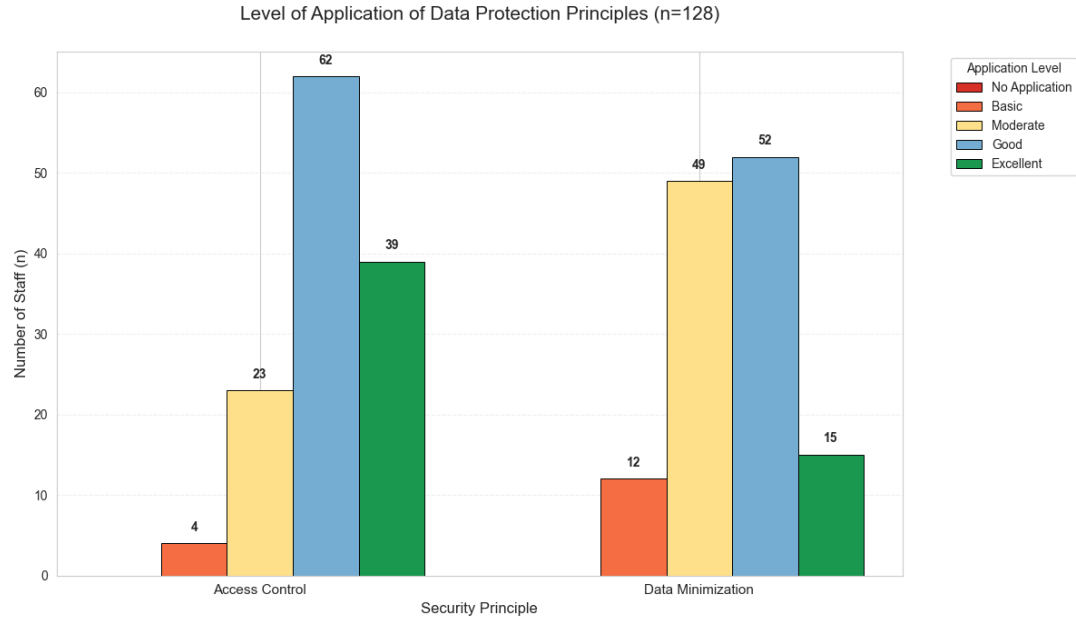


Figure 7: Application of Data Protection Principles (n=128)

As shown in figure 7, all the respondents reported that they apply access control with 62 respondents (48.4%) reporting that they perform good application, while 39 (30.5%) reported excellent application, 23 respondents (18.0%) reporting moderate application and 4 (3.1%) reporting basic application.

52 respondents (40.6%) reported to have good application of data minimization, 15 (11.7%) reported excellent application, 49 respondents (38.3%) reported moderate application, while 12 (9.4%) reported basic application.

4.5.4 Consistency of Protocol Adherence and Departmental Compliance

The study compared individual adherence to protocols with the perceived compliance of the hospital departments so as to evaluate the reliability of the data protection.

Table 11: Protocol Adherence and Departmental Compliance Ratings (n=128)

Assessment Metric	Frequency (n)	Percentage (%)
Departmental Compliance Rating		
Excellent	8	6.2%
Good	112	87.5%
Fair	8	6.2%
Poor	0	0.0%
Frequency of Following Protocols		
Rarely	27	21.1%
Sometimes	85	66.4%
Often	3	2.3%
Always	13	10.2%

Table 11 shows that the majority of the respondents (87.5%) rated their department's compliance with data protection rules as good, 6.2% rated it as excellent, 6.2% rated compliance as fair and no respondents rated their department as poor.

10.2% of staff reported that they always follow the data protection protocols, 2.3% follow them often, 66.4% follow them sometimes and 21.1% follow them rarely.

4.5.5 Primary Challenges to Effective Data Protection

Respondents indicated the barriers they encounter which could be hindering them from effectively protecting the patient health data on the digital health solutions.

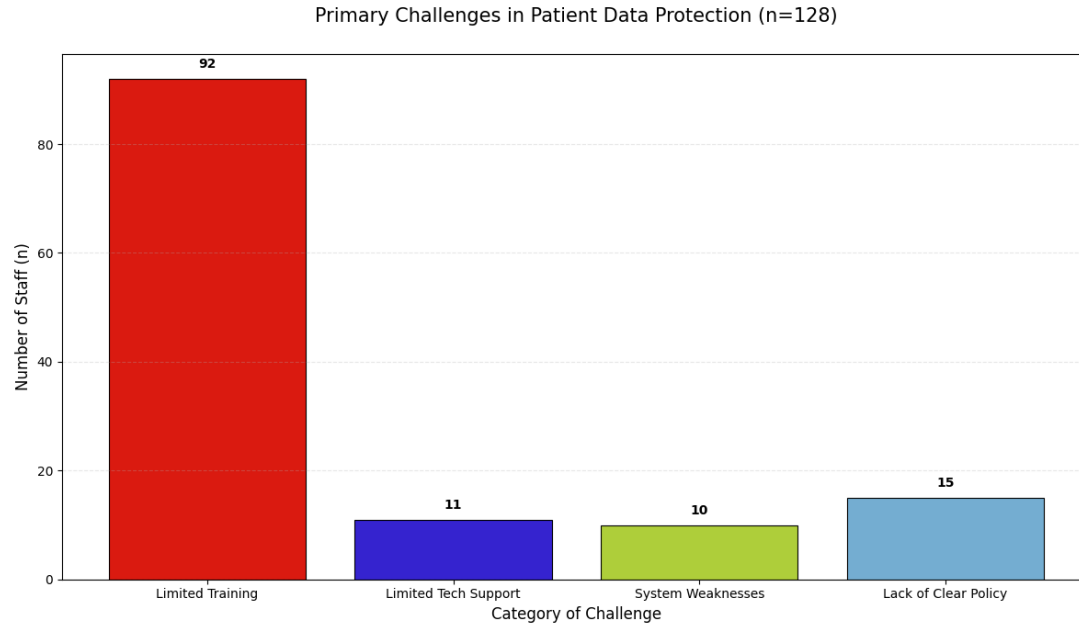


Figure 8: Primary Challenges to Effective Data Protection (N=128)

Among the respondents, the challenge of limited training was cited by 71.9% (n=92), lack of clear policy was reported by 15 healthcare workers, 10 respondents recorded system weaknesses and 11 respondents identified limited technical support and system weaknesses as the primary challenges.

4.5.6 Multiple Linear Regression Analysis of Digital Health Usage and Knowledge of Principles on Patient health data Protection Practices

Table 12: Multiple Linear Regression Analysis of Digital Health Usage and Knowledge of Principles on Patient health data Protection Practices

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.427 ^a	0.182	0.169	1.718
ANOVA ^b				

Model		Sum of Squares	df	Beta (β) / MS	t/F	Sig.(p)
1	Regression	82.092	2	41.046	13.899	.000*
	Residual	369.150	125	2.953		
	Total	451.242	127			
Coefficients^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t/F	Sig.(p)
		B/SS	Std. Error	Beta (β) / MS		
1	(Constant)	4.665	1.042		4.478	.000
	Digital Health Tools Usage	0.623	0.172	0.307	3.618	.000*
	Knowledge of Patient health data Protection Principles	0.116	0.045	0.219	2.580	0.011*
a. Predictors: (Constant), Digital Health Usage, Knowledge of Patient health data Protection Principles						
b. Dependent Variable: Patient health data Protection Practices						

P<0.05

A multiple linear regression analysis was conducted to study the effect of Digital Health Tools Usage and Knowledge of Patient health data Protection Principles on Patient health data Protection Practices. The overall model was statistically significant ($F(2, 125) = 13.899$, $p < 0.001$), with an R^2 of 0.182 which shows that the two predictors explained 18.2% of the variation in patient health data protection practices among the staff.

Digital Health Tools Usage was a significant positive predictor ($\beta = 0.307$, $p < 0.001$), showing that higher usage of digital health tools is associated with better patient health data protection practices. Also, Knowledge of Patient health data Protection Principles was a significant positive predictor ($\beta = 0.219$, $p = 0.011$) showing that greater knowledge of data protection principles is linked to higher adherence to patient health data protection practices and the constant of the regression model was 4.665 ($p < 0.001$).

4.6 Qualitative Analysis of Data Protection Practices

Qualitative interviews and field observations were conducted to provide a deeper understanding of the patient health data protection practices among the healthcare workers when using digital health solutions at Hoima Regional Referral Hospital plus the challenges these healthcare workers do face. In line with the study's sequential design, these qualitative results serve to elaborate on the statistical results by revealing the behavioural and structural reasons behind the identified data protection gaps.

4.6.1 Access Control and the convenience vs security Experience

The quantitative results in section 4.5.1 showed that while staff utilize passwords, session management which is logging out immediately after patient health data entry and utilization is significantly low. The qualitative data revealed that this is driven by a culture of credential convenience in that healthcare workers prefer to use easy or shared login credentials because it helps them keep work moving smoothly and avoid delays in patient care.

One of the healthcare workers noted that; *“individual accountability is often bypassed for departmental efficiency as staff frequently share their account credentials with colleagues,*

particularly when the account holder is not physically present but data entry is required for a patient.”- Clinical Officer

To manage the burden of remembering multiple passwords, one of the healthcare workers confessed to using high-risk storage methods. She noted:

“We store our passwords in the computer to avoid forgetting as we have fear of losing them as well which means in case someone is to use her computer, they can just use my credentials and enter into her account and use it for whatever intent.”-Midwife

These interview responses were confirmed by field observations. The researcher observed a Medical Doctor leaving a computer workstation open and unlocked to attend to other duties, leaving patient health data fully displayed and accessible to any unauthorized person or stranger in the vicinity including the researcher.

4.6.2 Technical Awareness and Encryption Gaps

The quantitative phase revealed a near total absence of encryption practices (97.7%). The qualitative interviews sought to explain whether this was a resource issue or a result of basic technical awareness.

A key finding was that many staff are unfamiliar with the technical requirements of digital data protection. This was highlighted by one of the healthcare workers who candidly confessed:

“I have never even heard about encryption.”- Lab Technician

Participants indicated that because the E-Afya system does not mandate encryption for internal transfers, they do not perceive it as a personal responsibility. The lack of practice is therefore a result of both a lack of tools and a lack of technical training.

4.6.3 Data Sharing, Consent and Assumed Consent

The interviews further explained why Data Minimization and Consent protocols are underutilized.

Regarding data sharing, a recurring theme was that staff view a patient's presence in the hospital as complete consent for all internal data processing. One of the healthcare workers explained this logic:

"We don't normally ask patients to consent because we assume that since the patient has come needing a check-up, they are already allowing us to make use of the patient health data to make further decisions." - Lab Technician

There is a general perspective that formalizing consent for every internal referral would slow down life-saving care, leading staff to prioritize clinical speed over the requirements of the Data Protection and Privacy Act (2019).

4.6.4 System Reliability and Departmental Silos

The quantitative results identified Limited Training (71.9%) and technical issues as primary challenges. The qualitative phase revealed that these challenges are intensified by system instability and the hospital's rotation policies.

A significant vulnerability was identified regarding system reliability and one of the healthcare workers explained that when the digital network fails, staff are forced to bypass digital security entirely and revert to manual record keeping:

"When the network is off or the system is down, we resort to noting down the information in books of which the writing in books, the interns can as well do that." - Midwife

This suggests that downtime creates a security space where manual records are accessible to unauthorized individuals (interns) without the protection of digital access controls.

A Nurse explained that training on the E-Afya system is often conducted in silos per department. When staff are rotated to a different ward, they find that their previous training does not apply to the new department's specific view:

“The challenge is limited training because they train per department and yet they keep changing us the departments where we are to work and if you join after the training that was done you have missed, you have to find out for yourself how other departments use E-Afya.”

One of the healthcare workers said that they also need more technical support as he confessed that;

“There are only two technical personnel whom all the departments depend on and that in case of an issue like network, he is called upon and comes but sometimes if he is busy, he can delay come.” - Dentist

4.7 The Triangulation Matrix

To ensure the accuracy, depth and relevance, Table 13 summarizes how the qualitative results explain the quantitative results.

Table 13: Triangulation of Quantitative and Qualitative Results (n=128)

Statistical Result (The “What”)	Qualitative Theme (The “Why”)	Evidence from Interviews/Observations
69.6% Rarely/Never Logout Immediately after patient health data handling	Prioritization of Clinical Speed as staff view relogging as a time barrier.	The observation was that the Dr. left screen open and unattended with patient health data visible.
58.6% Rarely Change Passwords	Credential Sharing Culture as account credentials are shared to maintain continuity.	Clinical Officer confirmed sharing credentials when not in place.
97.7% Never Encrypt	Technical Awareness Gap that Encryption is not part of the staff's vocabulary.	Lab Technician said <i>“I have never even heard about encryption.”</i>
52.3% Good Consent Application	Assumed Consent Culture as seeking formal consent is viewed as redundant.	Lab Technician: <i>“We assume they are already allowing us to make use of the data.”</i>
7.8% System Weakness	Manual Reversion because downtime leads to insecure manual record keeping.	Midwife said that Network failure leads to use of books, which records can even be done by interns.

71.9% Report Limited Training	Departmental Training Silos as rotation makes training obsolete.	Nurse: Training is department specific; staff must find out on their own if they missed the training in the department he or she has been allocated.
-------------------------------	--	--

CHAPTER FIVE

DISCUSSION OF FINDINGS

5.1 Introduction

This chapter presents a discussion of the study findings in relation to existing literature, structured around the three objectives of the research.

5.2 Summary of findings

This section summarizes the findings and implications of the data according to the objectives of the study. This study aimed to identify the digital health solutions used by healthcare workers at Hoima Regional Referral Hospital, to assess the knowledge of patient health data protection principles among healthcare workers in Hoima Regional Referral Hospital using digital health solutions and to describe the patient health data protection practices of healthcare workers in the use of digital health solutions.

5.3 Demographics

Most participants in this study were female by sex, which may be explained by the large number of nurses and midwives in the hospital workforce. Nursing and midwifery professions tend to have higher female representation (Likis & King, 2020). The majority of participants were aged between 31 and 50 years. This age distribution is expected because many healthcare workers in this range have completed their professional training and are actively engaged in service. Fewer participants were below this age group, possibly because many younger individuals are still in training, while those above 50 years may be approaching retirement, considering that the retirement age in Uganda is 60 years (Muhanguzi, 2021)

Many participants worked in the maternity and outpatient departments, which typically handle a high volume of patients. These departments require more staff due to the demand for services. The busy nature of the maternity department may also reflect Uganda's relatively high fertility rates among the Ugandan women (Kizza & Wasswa, 2024). According to the Uganda Demographic and Health Survey (UDHS) 2022, the total fertility rate (TFR) in Uganda is 5.2 children per woman, calculated among women of reproductive age (15-49 years) (Uganda

Bureau of Statistics [UBOS] & ICF, 2023. Most respondents had between four and ten years of work experience and held diploma qualifications since most of the nurses and midwives in Uganda have Diploma Education levels (Mbalinda et al., 2024)

5.4 Discussion of the findings concerning digital health solutions used by healthcare workers at HRRH

Objective One aimed at identifying the digital health solutions used by healthcare workers at Hoima Regional Referral Hospital. The findings show that the main systems are UgandaEMR (E-Afya), HMIS/DHIS2, Electronic Health Records and Automated Laboratory Information Systems (ALIS).

UgandaEMR (E-afya) was the most widely used and primary tool for managing patient information across most clinical departments by doctors, nurses, midwives, clinical officers and dentists. The qualitative findings revealed that UgandaEMR (E-afya) is the most used because it is the tool supported by the ministry of health and is recognised as a government owned digital health platform, mostly used in referral hospitals for patient health data management which aligns with Heart et al. (2017) study that shows nationally supported EMR systems are often the main platforms in public hospitals because they are officially implemented and aligned with Ministry of Health guidelines.

HMIS/DHIS2 were used mainly by nurses and clinical officers who used it to do the reporting of patient health data which aligns with research showing that DHIS2 is primarily a reporting tool rather than a system for everyday patient care. Its use is often restricted to staff responsible for documentation and health system reporting.

Automated Laboratory Information Systems were used exclusively by laboratory technicians for handling specimens, running laboratory tests, entering and validating lab results, they also used UgandaEMR to share results with doctors, which shows that the systems are integrated to support workflow between the lab and clinical teams. Milburn et al., 2024 argued that the laboratory systems are used by the laboratory healthcare workers and the integration with EMRs is very important as it improves efficiency.

Electronic Health Records were only used by the records officers, which showed that some digital health solutions are used by specific departments as also Feldacker et al. (2023) show that

in many public hospitals, digital health solutions are normally based on the healthcare worker's role.

This is consistent with Agbeyangi and Lukose (2025) study in sub-Saharan Africa, which shows that telemedicine adoption is limited due to poor internet, lack of equipment and funding challenges.

The findings from the Bivariate Analysis of the relationship between training and healthcare workers' confidence in using digital health tools showed that staff who had received training reported higher levels of confidence compared to those who had not received training as only trained staff reported being very confident in using digital systems. When healthcare workers are trained, they are more comfortable using electronic systems and are more likely to use them correctly and consistently (Kuek & Hakkennes, 2020) as training improves both technical skills and understanding of system functions.

The findings showed that some healthcare workers who did not receive formal training still said they were confident in using digital health systems and yet from the interviews, it was clear that many of them learned while working and mostly from their colleagues at work especially if training had been done before they joined that particular department. Others said they became confident simply by using the system many times. Benson (2019) shows that when people are using the digital health solutions more frequently, they can build confidence even if they have not received training.

The results also showed that the healthcare workers who were not trained did not have very high confidence which shows that they cannot fully implement the patient health data protection practices if they do not feel confident a certain way in using the digital health solutions.

The results from Spearman's correlation showed a moderate negative relationship between age and technical confidence meaning that the older healthcare workers were generally less confident in using the digital health solutions than the younger healthcare workers, a finding that makes sense because many younger healthcare workers were more exposed to using digital tools during their time of studying (Bezvikonnaya et al., 2024) of which today, many nursing schools teach basic computing to their students. Also, many older healthcare workers were trained when

patient records were written on paper and so moving from paper to digital health solutions can be difficult for them.

The interviews showed that there are challenges like the power cuts, poor internet connection in that when the network is down or there is no power, the healthcare workers resort to writing in books of which if these challenges take long, healthcare workers do not get enough time to practice using digital systems which can reduce confidence, especially for those who are already not comfortable with technology.

5.5 Discussion of the findings on Knowledge of Patient health data Protection Principles among healthcare workers at HRRH.

The findings showed that most healthcare workers at Hoima Regional Referral Hospital were not aware of the Uganda Data Protection and Privacy Act (2019) whereby only a few respondents said they knew about it which means that although staff handle patient information every day, many do not know the law that guides how patient data should be protected in Uganda.

The study also found that most healthcare workers had moderate knowledge of the patient health data protection principles where only a small number had very high or very low knowledge.

It shows that many healthcare workers understand the basic ideas about patient data privacy and handling information but they do not fully understand the legal rules and detailed principles and because their knowledge is not complete, there may be risks when handling the digital patient health data.

In many cases, healthcare workers depend more on what they learn through daily work experience than on formal legal guidelines so their moderate knowledge may come from regularly using digital systems and managing patient records. However, without formal training or clear guidance about the law, their understanding remains limited.

Low awareness and moderate knowledge can increase the risk of errors, data breaches or non-compliance with legal requirements. Swede et al. (2019) emphasize that formal training and awareness programs are necessary to ensure that healthcare workers understand both the

practical and legal aspects of patient health data protection. So, these findings show the need for training on the Data Protection and Privacy Act (2019), to strengthen both knowledge and compliance among healthcare staff.

These findings show that healthcare workers' knowledge varies across different data protection principles as staff demonstrated higher understanding of confidentiality, integrity and accountability as well as access control which suggests that healthcare workers are more familiar with principles that relate directly to everyday handling of patient information like keeping records secure, ensuring data is accurate and being responsible for patient health data.

In contrast, principles like informed consent and lawful usage had the lowest understanding indicating gaps in knowledge related to legal and ethical aspects of data protection, which require awareness of formal regulations and policies such as the Uganda Data Protection and Privacy Act (2019). Similarly, moderate understanding of Data Minimization and Availability shows that some staff may not fully appreciate best practices for limiting data collection or ensuring timely access to information.

These findings are consistent with literature showing that healthcare workers often understand practical data protection tasks better than legal or policy related principles (Spencer & Patel, 2019).

Studies as well indicate that gaps in knowledge about consent as some confessed that they do not normally ask patients to consent because they assume that since the patient has come needing a treatment or checkups, they are already allowing them to make use of the patient health data to make further decisions, lawful usage and data management policies can increase the risk of privacy breaches and non-compliance and this variation in knowledge across principles highlights the need for targeted training that focuses not only on general data protection practices but also on the legal and ethical requirements, so that healthcare workers can fully protect patient information.

Spearman's Rank Correlation findings from the relationship between demographic variables, knowledge and usage confidence showed that healthcare workers with more years of experience generally had lower knowledge and confidence levels.

Gender showed almost no relationship with knowledge, which suggests that both male and female healthcare workers have similar understanding of patient health data protection principles. However, there was a small difference in usage confidence whereby a weak but significant difference in usage confidence was observed across gender, with male healthcare workers reporting slightly higher confidence than females which may reflect variations in exposure or opportunities to interact with digital systems rather than differences in ability.

In some Ugandan hospitals, access to computers can depend on the duties which have been assigned to a healthcare worker, the shift patterns or the departmental roles, which may indirectly influence confidence in cases when some healthcare workers don't often use the digital solutions. Job title had a weak but significant relationship with knowledge implying that certain professional roles may provide more opportunities to learn about the digital health solutions and data protection for example records officers, laboratory technicians or department heads may interact more frequently with electronic reporting systems and so develop greater familiarity with them. On the other hand, job title did not significantly influence confidence which showed that even when knowledge differs slightly across roles, confidence in using the digital health solutions may depend more on individual experience and training than on job position alone.

Department did not as well show a significant relationship with either knowledge or confidence, implying that digital health solutions and data protection responsibilities were spread across departments in a relatively similar way in that whether a healthcare worker is in maternity, outpatient or another unit, they were expected to use digital health solutions and handle patient data in similar ways.

Education level showed only a weak relationship with both knowledge and usage confidence, in other words having a higher formal education does not necessarily mean that the healthcare workers have more knowledge of data protection principles or feel more confident using digital tools, thus showing that practical knowledge and experience are more important than formal education in influencing how confident they are when handling digital health systems.

5.6 Discussion of the findings on patient health data Protection Practices among healthcare workers at HRRH.

The findings showed that healthcare workers mostly rely on basic methods to protect patient health data like using passwords, some staff reported sharing credentials with their colleagues in case they are not on ground to access patient health data and make the necessary approvals which contradicts recommended security practices, logging out immediately after use of which the researcher observed instances where computers were left unlocked after use minus logging out even after entering the necessary patient health data and making the necessary approvals. More advanced measures like encryption or technical access restrictions were not used and key behaviours like regularly changing passwords or logging out immediately were often neglected as the qualitative results revealed that the healthcare workers do not change their account passwords regularly because they avoid forgetting them.

These practices can be explained through Protection Motivation Theory which suggests that people take protective actions when they perceive a threat and believe they can cope with it. In this study, while healthcare workers were aware of the importance of protecting patient health data this being the perceived threat, many lack the skills, training or system support to perform stronger protective actions which is the coping appraisal. And so, this then explains why the basic measures like passwords were used, but advanced protections such as encryption were absent as even some confessed that they have never heard of that and risky behaviours like leaving systems unlocked occur.

Qualitative insights support this interpretation as some staff stored passwords on computers to avoid forgetting them and computers were observed left unlocked with patient health data visible by the researcher which showed that they have less solid practices in protecting patient health data to ensure confidentiality. According to PMT, these behaviours occur when staff feel unable to fully control or cope with the threat, even if they understand its importance.

And so, the findings showed that patient health data protection depends not only on awareness but also on self-efficacy and system support. Strengthening protection therefore requires training to increase confidence, policies to encourage safe behavior and technical safeguards that make protective actions easier to perform.

In addition, the findings on application of technical and organizational principles showed that healthcare workers at Hoima Regional Referral Hospital applied technical and organizational principles of patient health data protection, particularly access control and data minimization to varying degrees since most staff reported moderate to good application, with fewer reporting excellent or basic application suggesting that while healthcare workers understand the importance of limiting access of patient records to only the authorized and collecting only necessary data, there are gaps in consistently applying these principles as even some confessed that they even share their credentials with their fellow staff members when they are not present physically at the Hospital.

These results can be interpreted through the Protection Motivation Theory used in this study which explains that protective actions are influenced by both the perceived threat and the perceived ability to cope. In this case, staff may recognize that possibility of unauthorized access from those very workmates they share with their credentials or excessive data collection is a risk, but their ability to fully implement access controls or enforce data minimization may be limited by system constraints, lack of training, workflow pressures or even ignorance.

The results from the multiple linear regression analysis showed that both using digital health tools and understanding patient health data protection principles affected how staff handle patient information. Staff who used digital tools regularly followed proper data protection practices more carefully and those with better knowledge of data protection principles applied these practices more consistently.

This suggests that hands-on experience with digital tools and a good understanding of data protection rules are important for keeping patient information secure. While other factors may also influence practices, providing training on using digital tools and increasing staff knowledge of data protection principles can help improve adherence to safe practices.

On the other hand, the findings also revealed the challenges that hinder the healthcare workers from having good patient health data protection practices when using the digital health solutions and these showed that main issues the healthcare workers faced were limited training, limited

technical support as some declared that sometimes support tends to delay and come after a day or two which affects their operation, system instabilities and lack of clear policies. These challenges were reported both quantitatively and qualitatively, showing that barriers occur at human, technical and organizational levels.

Limited training was the most commonly reported challenge as staff reported that they often received departmental training, so when a staff member who was not in that department say a nurse has been rotated from their current department to another department, they find it hard to interact with the systems that are used in another department because by they missed training that was already held in the department they are put in and so they had to learn the new system on their own which was hard for them. This finding aligns with literature showing that insufficient and fragmented training reduces staff confidence (Mandato & Kulhanek, 2022) and increases the risk of errors or unsafe practices.

System reliability issues further complicated data protection. Downtime forced staff to revert to manual records that is recording in books, which are less secure and accessible to unauthorized individuals. Observations and qualitative reports indicated that interns or other staff not fully qualified could access these records during system failures, creating temporary security vulnerabilities. Gromova, Koneva, and Titova (2022) stated that system instability is a major barrier to implementing digital security measures effectively.

Limited technical support and policy gaps also emerged as barriers since the healthcare workers reported that only a few technical personnel manage all digital systems and sometimes when they need system help, the technical support team can take long without coming through, so delays in resolving issues can compromise data protection.

Additionally, policies being unknown or not clear can reduce guidance on best practices, leaving staff to make inconsistent decisions. Oyetunji (2024) stated that organizational support, clear policies and adequate technical assistance are critical for ensuring compliance with data protection standards.

5.7 Study Limitations

This study had some limitations. Since the study was conducted at one point in time, it could only show relationships between variables but could not confirm whether one variable directly influenced another. In addition, the study used information provided by the respondents themselves. Some participants may not have given fully accurate answers because they forgot some information or wanted to provide answers that appeared acceptable or professional. Also, the study was conducted only at Hoima Regional Referral Hospital, therefore the findings may not fully represent healthcare workers in other hospitals or health facilities.

CHAPTER SIX

CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter presents the conclusions and the recommendations drawn from the findings of the study for improving the use of digital health solutions, knowledge of patient health data protection principles and patient health data protection practices among the healthcare workers at Hoima Regional Referral Hospital.

6.2 Conclusion

6.2.1 Digital Health Solutions Used at HRRH

Healthcare workers at Hoima Regional Referral Hospital primarily used UgandaEMR (e-Afya), HMIS/DHIS2, Electronic Health Records, and Automated Laboratory Information Systems (ALIS). The most commonly used digital health solution was the UgandaEMR-Eafya mainly used for managing patient information across the different departments in the Hospital.

6.2.2 Knowledge of Patient health data Protection Principles

Healthcare workers demonstrated moderate knowledge of patient health data protection principles for they were aware of practical measures like maintaining confidentiality, ensuring data integrity and access control using passwords as they all had user accounts. However, understanding of legal requirements was limited moreover with the majority of the healthcare workers not having knowledge of the Uganda Data Protection and Privacy Act, 2019.

6.2.3 Patient health data Protection Practices

Patient health data protection practices among healthcare workers were generally moderate to weak. While basic practices such as password use and system logout were observed, several risky behaviours and critical gaps in digital security practices were also identified, including password sharing and complete absence of encryption practices so, the findings indicated

insufficient compliance with advanced patient data protection standards in the Data Protection and Privacy Act, 2019 as some of the technical measures like encryption were not applied by the healthcare workers as some even confessed that they had never heard of it.

6.3 Recommendations

Based on the findings from this study, the researcher proposes the following recommendations to improve the way the digital health solutions are used, the knowledge of patient health data protection principles and the Patient health data protection practices among the healthcare workers at Hoima Regional Referral Hospital.

The study recommends that all healthcare workers should receive continuous hands-on training on how to use the digital health systems because this will also improve their confidence and so the healthcare workers will best learn how to apply the patient health data protection principles.

Hoima Regional Referral Hospital should develop, communicate simple, clear policies on system access, password management and patient health data handling because some of the healthcare workers confessed that it is possible that the policies are there but they simply didn't know them.

The study also proposes that reliable IT support should be recruited and should immediately come through when called upon to prevent frustration among the health care workers because this will add more bias among the healthcare workers towards using digital health solutions, stable internet connectivity as sometimes when network is off, they cannot be able to use the digital health solutions to further perform clinical tasks. Also, backup power systems should be put in place because when electricity off, digital health solutions cannot be used which forces healthcare workers to use the manual systems for record keeping.

Workshops and awareness campaigns should be held in the hospital so as to educate the healthcare workers on the Uganda Data Protection and Privacy Act (2019) and any other relevant guidelines because, ensuring that the staff understand their legal obligations will strengthen compliance to the patient data protection protocols and reduce the risk of data breaches.

Lastly, further studies could examine the impact of the training programs on healthcare workers' technical confidence and data protection compliance to the necessary protocols, explore the feasibility of digital health solutions usage in regional referral hospitals since this study was particularly done at HRRH and as well find out how system usability and support influence secure handling and maintenance of patient health information.

REFERENCES

- Agbeyangi, A. O., & Lukose, J. M. (2025, March). Telemedicine adoption and prospects in sub-Saharan Africa: a systematic review with a focus on South Africa, Kenya, and Nigeria. In *Healthcare* (Vol. 13, No. 7, p. 762). MDPI.
- Akter, S., Mohiuddin Babu, M., Hossain, M. A., & Hani, U. (2021). How does value co-creation transform quality of life at the bottom of the pyramid? *Journal of Marketing Management*, 37(9-10), 962-992.
- Alunyu, A. E., Amiyo, M. R., & Nabukenya, J. (2024). Contextualised digital health communication infrastructure standards for resource-constrained settings: Perception of digital health stakeholders regarding suitability for Uganda's health system. *PLOS Digital Health*, 3(9), e0000603.
- Astaneh, B., Raeisi Shahraki, H., Astaneh, V., & Guyatt, G. (2024). Effective hands-on teaching strategy on participants' confidence in medical writing and publishing: A before-after study. *Plos one*, 19(7), e0307681.
- Babughirana, G., Nsumba, J. F., Nangosha, E., Musasizi, B., Mulindwa, R. M., Manyasi, B., & Adeke, L. Electronic Supported Solutions to Scale-up Maternal New-born and Child Health Interventions Feasibility Assessment for Hoima District.
- Bagyendera, M., Nabende, P., & Nabukenya, J. (2023). Critical factors influencing data use and utilization in health systems: a focus on data and interoperability standards for health information exchange (HIE) in Uganda's health care system. *Oxford Open Digital Health*, 1, oqad015.
- Bărcanescu, E. D. (2021). Cybersecurity and Data Protection in Healthcare: A Review of the Regulatory Frameworks. *Journal of Healthcare Management*, 66(2), 132-142.

Benson, T. (2019). Digital innovation evaluation: user perceptions of innovation readiness, digital confidence, innovation adoption, user experience and behaviour change. *BMJ health & care informatics*, 26(1), e000018.

Bezvikonnaya, E., Bogdashin, A., & Portnyagina, E. (2024). The use of digital technologies in the practice of adaptation of young professionals.

Bostan, S., Johnson, O. A., Jaspersen, L. J., & Randell, R. (2024). Contextual Barriers to Implementing Open-Source Electronic Health Record Systems for Low-and Lower-Middle-Income Countries: Scoping Review. *Journal of Medical Internet Research*, 26, e45242.

Chief Healthcare Executive. (2023). Nearly 50 million Americans impacted by health data breaches in 2022. *Chief Healthcare Executive*.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Determann, L. (2019). Healthy data protection. *Mich. Tech. L. Rev.*, 26, 229.

Elger, B. S., et al. (2014). Security and privacy in the digital healthcare system: A literature review. *Journal of Medical Internet Research*, 16(12), e240.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, 30(2), 407-429.

Feldacker, C., Mugwanya, R., Irongo, D., Kathumba, D., Chiwoko, J., Kitsao, E., ... & Tweya, H. (2023). A community-based, mobile electronic medical record system app for high-quality, integrated antiretroviral therapy in Lilongwe, Malawi: design process and pilot implementation. *JMIR Formative Research*, 7, e48671.

Gulnoza, K., & Niginabonu, K. (2022). Questionnaire and Its Application. *Research Focus*, 1(3), 78-82.

Gebeyew, A. S., Zemene, W., Tilahun, B. C., Mengestie, N. D., Endehabtu, B. F., Wordofa, Z. R., ... & Sisay, M. M. (2025). Digital health data security practices among health professionals in low-resource settings: cross-sectional study in Amhara Region, Ethiopia. *BMC Medical Informatics and Decision Making*, 25(1), 60.

Gromova, E. A., Koneva, N. S., & Titova, E. V. (2022). Legal barriers to the implementation of digital industry (Industry 4.0) components and ways to overcome them. *The Journal of world intellectual property*, 25(1), 186-205.

Groenewald, T. (2004). A phenomenological research design illustrated. *International journal of qualitative methods*, 3(1), 42-55.

Govender, M., 2022. Digital health applications used by community health workers for the management of HIV/AIDS and TB in the southern African development community region: A scoping review on the factors that influence the success and failure of such applications.

Heart, T., Ben-Assuli, O., & Shabtai, I. (2017). A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. *Health Policy and Technology*, 6(1), 20-25.

https://media.ulii.org/media/legislation/18002/source_file/b6ae5cce4290322a/2019-9.pdf

Kizza, J., & Wasswa, G. (2024). Education and Fertility preference among women in Uganda. *Tanzania Journal of Health Research*, 25(3).

Kuek, A., & Hakkennes, S. (2020). Healthcare staff digital literacy levels and their attitudes towards information systems. *Health informatics journal*, 26(1), 592-612.

Kayondo, B. N., & Kyobe, M. (2025). The Influence of Self-Efficacy, Trust, Perceived Costs and Healthcare-Environment on Compliance with the Data Protection and Privacy Act by Health

Workers in Uganda. *The Electronic Journal of Information Systems in Developing Countries*, 91(2), e70002.

Khatiwada, P., Yang, B., Lin, J. C., & Blobel, B. (2024). Patient-Generated Health Data (PGHD): Understanding, Requirements, Challenges, and Existing Techniques for Data Security and Privacy. *Journal of Personalized Medicine*, 14(3), 282.

Kwesigabo, E. M., & Komba, L. I. (2025). Patient health data Protection in Healthcare: A Comprehensive Assessment of Cybersecurity Best Practices among System End-Users. A Case of Peramiho Mission Hospital. *European Journal of Applied Science, Engineering and Technology*, 3(3), 360-371.

Likis, F. E., & King, T. L. (2020). Gender diversity and inclusion in midwifery. *J Midwifery Womens Health*, 65(2), 193-194.

Mbalinda, S. N., Livingstone, K., Najjuma, J. N., Gonzaga, A. M., Lusota, D., Musoke, D., & Owusu-Sekyere, S. (2024). Fostering professional identity formation and motivation for joining nursing and midwifery programmes among undergraduate nursing/Midwifery students and recent graduates in Uganda. *Annals of Global Health*, 90(1), 61.

Masrom, M. (2007). Technology acceptance model and e-learning. *Technology*, 21(24), 81.

García-Avilés, J. A. (2020). Diffusion of innovation. *The international Encyclopedia of media psychology*, 1(8).

Mensah, N. K., Adzakupah, G., Kissi, J., Taylor-Abdulai, H., Johnson, S. B., Agbeshie, P. A., ... & Boadu, R. O. (2024). Health professionals' ethical, security, and patient safety concerns using digital health technologies: a mixed method research study. *Health Services Insights*, 17, 11786329241303379.

- Milburn, J., Turner, P., Kehrer, S., & Badrick, T. (2014). Redesigning workflow and staff competencies to deal with staff shortages in a regional laboratory. *Australian Journal of Medical Science*, 35(1), 16-21.
- Mandato, K., & Kulhanek, B. (2022). The impact of inadequate training. In *Healthcare Technology Training: An Evidence-based Guide for Improved Quality* (pp. 11-17). Cham: Springer International Publishing.
- Moore, W., & Frye, S. (2019). Review of HIPAA, part 1: history, protected health information, and privacy and security rules. *Journal of nuclear medicine technology*, 47(4), 269-272.
- Muhanguzi, K. B. (2021). Pensions and Timing of Retirement: The Case of the Public Service Pension Scheme in Uganda. *Available at SSRN 3874784*.
- Mukobi, P., 2018. Service delivery and customer satisfaction in public hospitals in Uganda: A case study of Hoima Regional Referral Hospital (Doctoral dissertation, Nkumba University).
- Mudogo, C., Mulwa, A., Kyalo, D. and Mwangi, C., 2023. Enhancing Performance of HIV/AIDS Projects through Digital Health Interventions for Client Appointments in Kisumu County, Kenya. *European Journal of Theoretical and Applied Sciences*, 1(4), pp.618-629.
- Mutebi, J., Kareyo, M., Chinecherem, U., Muhaise, H., Akampurira, P., & Okello, M. (2022). Medical information breaches occurrence with respect to Social Media usage, in selected medical institutions in Uganda. *Journal of Computer and Communications*, 10(10), 10-3
- Namatovu, H. K., Semwanga, A. R., Kiberu, V. M., Ndigezza, L., Magumba, M. A., & Kyanda, S. K. (2021, December). Barriers and facilitators of eHealth adoption among healthcare providers in uganda—a quantitative study. In *International Conference on e-Infrastructure and e-Services for Developing Countries* (pp. 234-251). Cham: Springer International Publishing.
- Nasrabadi, A. N., Norouzkhani, N., Manookian, A., Cheraghi, M. A., Mohammadi, M., Izadidastenaeei, Z., & Goudarzian, A. H. (2024). Safeguarding Patient Information as an Issue Faced by Nurses: A policy brief. *Asia Pacific Journal of Health Management*, 19(2).

Nagwovuma, M., Ndagire, L., & Eilu, E. (2021, May). Performance Evaluation for electronic health information systems in Uganda. In *2021 IST-Africa Conference (IST-Africa)* (pp. 1-8). IEEE.

Ogbodo, D. C., Awan, I. U., Cullen, A., & Zahrah, F. (2025). From Regulation to Reality: A Framework to Bridge the Gap in Digital Health Data Protection. *Electronics*, *14*(13), 2629.

Oyetunji, S. A. (2024). Investigating Data Protection Compliance Challenges. *Int. J. Innov. Sci. Res. Technology. (IJISRT)*, *9*, 17.

Parthasarathy, R., Rangarajan, A., & Garfield, M. J. (2021). Implementation of secure health information technology innovations: An extended diffusion of innovations perspective. *e-Service Journal*, *12*(3), 43-76.

Singh, I., & Singh, Y. A. S. H. I. K. (2022). Cyber-security knowledge and practice of nurses in private hospitals in northern Durban, kwazulu-Natal. *Journal of Theoretical and Applied Information Technology*, *100*(1), 246-267.

Shah, S. I. (2020). Data Breaches in Healthcare: A Rising Concern. *International Journal of Health Security*, *45*(1), 15-22.

Sittig, D. F., et al. (2016). Protecting Health Information: Current Challenges and Solutions. *Journal of the American Medical Informatics Association*, *23*(6), 1245-1250.

Swede, M. J., Scovetta, V., & Eugene-Colin, M. (2019). Protecting patient health data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. *Journal of allied health*, *48*(2), 148-156.

Spencer, A., & Patel, S. (2019). Applying the data protection act 2018 and general data protection regulation principles in healthcare settings. *Nursing Management*, *26*(1).

Takuwa, M., Mbabazi, S. E., Tusabe, M., Mulindwa, B., Makobore, P. N., Mulerwa, M., ... & Ssekitoleko, R. T. (2023). Mobile health access and utilisation in uganda: knowledge, attitudes and perceptions of health and veterinary workers. *Telemedicine and e-Health*, 29(6), 912-920.

Turkstani, H. A., Almutawah, F. N., AlZamel, N. A., Zaid, M., Alshammari, A. A. A., Algharbi, M. T., ... & Aljuwayed11, N. H. (2025). Privacy and Confidentiality in Healthcare: Best Practices for Protecting Patient Information. *J. Healthc. Sci*, 5.

Tumuhimbise, W., Atwine, D., Kaggwa, F., & Musiimenta, A. (2023). Acceptability and feasibility of a mobile health application for enhancing public private mix for TB care among healthcare Workers in Southwestern Uganda. *BMC Digital Health*, 1(1), 9.

Uganda Bureau of Statistics (UBOS), & ICF. (2023). *Uganda Demographic and Health Survey 2022 final report*. Kampala, Uganda, and Rockville, Maryland, USA: UBOS and ICF.

Williams, M. D., Rana, N. P., & Dwivedi, Y. K. (2015). The unified theory of acceptance and use of technology (UTAUT): a literature review. *Journal of enterprise information management*, 28(3), 443-488.

Westin, A. F. (2003). Privacy and Freedom. Atheneum Press.

Perkel, J. M. (2018). Critical security flaws found in OpenEMR, an open-source electronic health records system. TechCrunch

Weik, L., Fehring, L., Mortsiefer, A., & Meister, S. (2024). Understanding inherent influencing factors to digital health adoption in general practices through a mixed-methods analysis. *Npj Digital Medicine*, 7(1), 47.

Yeng, P. K., Fauzi, M. A., & Yang, B. (2022). A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals. *Information*, 13(7), 335.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publication.

APPENDICES

APPENDIX 1: HEALTHCARE WORKER RESEARCH QUESTIONNAIRE

A questionnaire on healthcare workers' knowledge of patient health data protection when using digital health solutions at Hoima Regional Referral Hospital

Dear Participant,

This questionnaire aims to collect information on your knowledge and practices regarding patient health data protection when using digital health solutions. Your responses was treated confidentially and was used only for academic purposes. Please answer all questions honestly by ticking the appropriate option or providing the requested information. Filling in this questionnaire might take you about 10-15 mins.

DEMOGRAPHIC INFORMATION

1. Age in complete years (e.g 40 years): _____

2. Gender:

- ☐ Male
☐ Female

3. Department:

- ☐ OPD
☐ Maternity
☐ Laboratory
☐ All departments
☐ Surgery
☐ Gynaecology
☐ ICU
☐ Medical ward
☐ Dental Department

☐ Other: _____

4. Job title:

☐ Medical Doctor

☐ Nurse

☐ Record Officer

☐ Lab Technician

☐ Clinical officer

☐ Midwives

☐ Dentist

☐ Other: _____

5. Years of experience:

☐ Less than 1 year

☐ 1 to 3 years

☐ 4 to 6 years

☐ More than 6 years

☐ Other: _____

6. Years of working in the current station

☐ Less than 1 year

☐ 1 to 3 years

☐ 4 to 6 years

☐ More than 6 years

☐ Other: _____

7. Level of Education:

☐ Certificate

☐ Diploma

☐ Bachelor's Degree

☐ Master's Degree

- ☐ PhD
- ☐ Other _____

RQ1: THE DIGITAL HEALTH SOLUTIONS USED

This checklist serves as a guide for identifying the most common digital health solutions utilized by healthcare workers at Hoima Regional Referral Hospital.

Please tick (✓) the digital health solutions you use in your work and provide a brief description of their purpose and how often you use them.

1. Which of the following digital health tools do you use? (Select all that apply)

- ☐ Electronic Health Records (EHR)
- ☐ Health Management Information System (HMIS)
- ☐ District Health Information System 2 (DHIS2)
- ☐ Electronic Medical Records-UgandaEMR
- ☐ Automated Laboratory Information System
- ☐ Telemedicine Platform
- ☐ Online Software
- ☐ Other (please specify): _____

2. In which areas of your work do you make use of digital health solutions? (Select all that apply)

- ☐ Patient health data record keeping
- ☐ Appointment scheduling
- ☐ Diagnosis support
- ☐ Reporting and statistics
- ☐ Communication with Patients
- ☐ Communication with other Departments/Staff
- ☐ Clinical documentation
- ☐ Others (please specify) _____

3. In your daily duties, what specific tasks or activities do these digital health solutions help you perform?

- ☐ Patient registration
- ☐ Clinical documentation
- ☐ Reporting & statistics
- ☐ Communication with patients/staff
- ☐ Other (specify) _____

4. How often do you use digital health solutions?

- ☐ Daily/All the time
- ☐ Weekly
- ☐ Occasionally
- ☐ Rarely
- ☐ Not at all

5. In which department do you mainly use these digital health solutions?

- ☐ OPD
- ☐ Maternity
- ☐ Laboratory
- ☐ All departments
- ☐ Surgery
- ☐ Gynaecology
- ☐ ICU
- ☐ Medical ward
- ☐ Dental Department
- ☐ Other (please specify) _____

6. How would you rate your confidence in using digital health solutions?

- ☐ 1(Not confident at all)
- ☐ 2 (Somewhat not confident)
- ☐ 3 (Neutral)

- ☐ 4 (Confident)
- ☐ 5 (Very confident)

2 Have you ever received any training on patient health data protection and privacy when using digital health solutions?

- ☐ Yes
- ☐ No

RQ2: KNOWLEDGE OF PATIENT HEALTH DATA PROTECTION PRINCIPLES

1. Are you aware of the Data Protection and Privacy Act, 2019 in Uganda?

- ☐ Yes
- ☐ No

2. Which of the following do you understand and apply as patient health data protection principles? (Rate on a scale of 1-5: 1 = No Understanding, 2 = Basic Understanding, 3 = Moderate Understanding, 4 = Good Understanding, 5 = Excellent Understanding))

Patient health data Protection Principle	1(N)	2(B)	3(M)	4(G)	5(E)
Confidentiality (keeping patient health data private and secure)					
Integrity (ensuring data is accurate and complete)					
Availability (ensuring data is accessible to authorized personnel when needed)					
Accountability (responsibility for data handling practices)					
Consent (patients agreeing before their data is shared)					
Lawful and fair processing (using data only for legitimate purposes)					
Access control					
Data minimization (Don't collect or store more patient information than you actually need)					

3. In your opinion, how important is patient health data confidentiality when using digital health solutions?

- ☐ Very important
- ☐ Important
- ☐

Neutral

☐ Not important

4. When entering or using patient health data, which of the following actions do you take to ensure the accuracy and completeness of the information? (Tick all that apply)

Accuracy (correctness of data):

- ☐ Restricting unauthorized edits
- ☐ I double-check patient information before entering it into the system
- ☐ I cross-verify information with patient records or other sources
- ☐ I review previous entries for errors
- ☐ I use system validation checks (e.g., mandatory fields, error messages)
- ☐ Other (please specify): _____

Completeness (making sure that all required information is recorded):

- ☐ I ensure all required fields in the system are filled before saving
- ☐ I follow a checklist or standard protocol for data entry
- ☐ I update missing information as soon as it becomes available
- ☐ I request missing information from colleagues or patients
- ☐ Other (please specify): _____

5. Do you obtain patient consent before sharing their information with other departments or third parties?

- ☐ Always
- ☐ Sometimes
- ☐ Rarely
- ☐ Never

6. Which security measures are you aware of that protect patient health data in digital systems? (Tick all that apply)

- ☐ Password protection
- ☐ User access control (role-based access)
- ☐ Data encryption
- ☐ Regular data backups
- ☐ Audit trails (tracking user activity)

☐ Other (specify) _____

7. Which of the following data security measures help to protect patient health data in digital systems do you have knowledge about as you work with patient health data? (*Tick all that apply*)

- ☐ Password protection
- ☐ Role-based access control (only authorized staff access records)
- ☐ Data encryption during storage and transfer
- ☐ Regular data backups
- ☐ Secure disposal of outdated records
- ☐ Audit trails/logs to monitor access

8. Do you think healthcare workers at Hoima RRH are sufficiently knowledgeable about patient health data protection?

- ☐ Yes
- ☐ No
- ☐ Not sure

9. On a scale of 1-5, indicate your level of agreement with the following statements about your knowledge of patient health data protection. (1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

Statement	1(SD)	2(D)	3(N)	4(A)	5(SA)
I understand the basic principles of patient health data privacy, such as confidentiality, informed consent, data minimization and secure data sharing					
I am aware of access control measures used to protect patient health data.					
I know how patient consent affects data sharing practices					
I understand the common digital risks to patient health data like hacking, unauthorized access					
I am familiar with policies and laws related to patient health data protection in this hospital.					

10. Do you feel equipped to handle data protection challenges like preventing data breaches, protecting patient confidentiality in your current role?

- ☐ Yes, I feel well-equipped
- ☐ Somewhat equipped, but I need more training
- ☐ No, I do not feel equipped

11. Which of the following patient health data protection measures are you confident in applying? (Select all that apply)

- ☐ Encrypting sensitive data
- ☐ Using strong passwords or authentication methods
- ☐ Limiting access to patient records based on roles
- ☐ Reporting suspected breaches or security issues
- ☐ None of the above

12. How would you rate your department's compliance with data protection standards when using digital systems?

- ☐ Excellent
- ☐ Good
- ☐ Fair
- ☐ Poor

13. What challenges do you face in maintaining patient health data protection when using digital systems?

- ☐ Lack of training
- ☐ Limited technical support
- ☐ System weaknesses
- ☐ Lack of clear policy
- ☐ Other: _____

14. How do you protect patient health data when using digital health systems?

- ☐ Use of passwords or login credential
- ☐ Regularly logging out of the system after use
- ☐ Avoiding sharing login details
- ☐ Encrypting or restricting file access
- ☐ None of the above

Are there areas where you feel your knowledge of patient health data protection principles is insufficient? (Specify) _____

RQ3: PATIENT HEALTH DATA PROTECTION PRACTICES

Please indicate how often you perform the following practices when using digital health solutions in the checkbox. (1 = Never, 2 = Rarely, 3 = Sometimes, 4 = Often, 5 = Always)

1. Access Control and Authentication

Statement	1(Never)	2(Rarely)	3(Sometimes)	4(Often)	5(Always)
I use strong passwords and change them regularly.					
I limit access to patient health data only to authorized persons.					
I log out immediately after using digital health systems					

2. System and Data Integrity

Statement	1(Never)	2(Rarely)	3(Sometimes)	4(Often)	5(Always)
I encrypt the patient health data because it is confidential.					
I ensure patient health data is accurate and complete before entering it into a digital health system					
I only share patient health data using secure and approved channels like encrypted hospital networks, not personal email					

I often send and receive patient health data using an unencrypted platform like personal email or WhatsApp?					
I only share encrypted patient health data because it is confidential to prevent unauthorized access.					

3. Physical and Device Security

Statement	1(Never)	2(Rarely)	3(Sometimes)	4(Often)	5(Always)
I ensure devices used for digital health solutions are secure, for example, by locking screens and having them password-protected					
I avoid storing patient health data on my personal mobile phone or computer					
I dispose of patient health data on electronic devices like phones, tablets in a secure manner					

4. Reporting and Compliance

Statement	1(Never)	2(Rarely)	3(Sometimes)	4(Often)	5(Always)
I access patient records only when it is necessary for your clinical task?					
I report any incidents of suspected patient health data breaches to my supervisor or the IT department					
I am familiar with the Uganda Data Protection and Privacy Act, 2019 and its relevance to my work					
I have received formal training from the hospital on patient health data protection.					

5. Organizational and Infrastructural Support

Statement	1(Never)	2(Rarely)	3(Sometimes)	4(Often)	5(Always)
The hospital provides clear, written policies on how to handle patient health data securely.					
The digital health systems I use are reliable and function correctly.					
The internet and electricity supply at the hospital are reliable enough to allow me to use digital health systems securely and consistently					

CHALLENGES IN DATA PROTECTION

1. How often do you follow patient health data protection protocols when using digital health solutions?

- ☐ Never
☐ Rarely
☐ Sometimes
☐ Frequently
☐ Always

2. What challenges do you face in ensuring patient health data protection?

- ☐ Lack of training
☐ Limited resources
☐ System vulnerabilities
☐ Lack of institutional policies
☐ Other (please specify) _____
☐ None

3. How effective do you think the hospital's digital health solutions are in protecting patient health data?

- ☐ Very in effective
☐ Ineffective

- ☐ Neutral
- ☐ Effective
- ☐ Very effective

4. What challenges do you face regarding patient health data protection in using digital health solutions? _____

5. What recommendations do you have to improve patient health data protection practices in this hospital? _____

APPENDIX 2: HEALTHCARE WORKER INTERVIEW GUIDE

Interview Guide for Exploring Healthcare Workers' Knowledge, Practices, and Challenges in Patient Health Data Protection Using Digital Health Solutions at Hoima Regional Referral Hospital

Introduction

I greet you all, my name is Jacqueline Ainabyoona, a Master's student of Public Health from Uganda Christian University conducting this research to explore healthcare workers' knowledge of patient health data protection when using digital health solutions. This interview should take about 10-25 minutes.

Please be assured that all the information you share will be kept completely confidential in that your name will not be used in my research and your identity will remain private.

Before we begin, do I have your consent to proceed with the interview? Do I also have your permission to audio-record this session to ensure I don't miss any important details? The recording will be for my use only and will be deleted after the research is complete.

Interview Questions

DEMOGRAPHIC INFORMATION

Thank you. Just for my records, I'd like to ask a few quick questions about your background.

1. Kindly state your job title?

2. How many years of experience do you have in this field of dealing with patient health data?

3. For how long have you worked at Hoima Regional Referral Hospital?

4. In which department do you work?

5. What is your highest level of education? _____

6. Gender: _____

RQ 3: PATIENT HEALTH DATA PROTECTION PRACTICES

A. Access Control & Authentication

7. How do you ensure that only authorized personnel access patient health data? Some of the examples are user accounts, role-based access, password protection, multi-factor authentication.

8. How often do you change passwords or follow other authentication protocols?

B. Data Integrity & Accuracy

9. How do you make sure that patient health data is accurate, complete, and not tampered with?

examples include double-checking entries, audit trails, system validation checks

C. Data Confidentiality & Security

10. What measures do you use to keep patient health data confidential when stored or transmitted digitally? For example, encrypting files, secure sharing platforms, avoiding personal emails or messaging apps

D. Data Storage & Backup

11. How is patient health data stored safely in your department? _____

12. Are there regular backups of patient records? How do you participate in ensuring backups are done? _____

E. Data Sharing & Consent

13. How do you share patient health data with colleagues, other departments, or external providers while ensuring confidentiality and consent? _____

14. How do you ensure that the patient has been given consent before their data is shared?

F. Monitoring & Reporting

15. Have you ever observed or reported any data breaches, unauthorized access, or mishandling of patient information?

16. What steps do you follow when a potential breach occurs? _____

G. CHALLENGES AND RECOMMENDATIONS

17. What challenges do you face in implementing patient health data protection practices?

18. What type of support, resources, or training would help you improve patient health data protection in your work?

Closing

Is there anything else you would like to share about protecting patient health data when using digital health solutions? _____

Thank you very much, dear participant for your valuable insights.

APPENDIX 3: COMMON DIGITAL HEALTH SOLUTIONS

This appendix provides a list of common digital health solutions used by healthcare workers in Uganda. This list serves as a reference for the study's findings, aligning with the first research objective to identify the digital health solutions used at Hoima Regional Referral Hospital.

1. Electronic Medical Records (EMRs), used for managing comprehensive patient health information, including diagnoses, treatments, and prescriptions. An example is the UgandaEMR system.
2. District Health Information Systems (DHIS2), widely used data platform for collecting, analysing and reporting routine health data, particularly for surveillance and public health planning.
3. Health Management Information Systems (HMIS), a broad category of systems for managing health facility-level data, often referred to as the Integrated Health Facility Management Information System (iHFMIS) in Uganda.
4. Community Health Worker (CHW) Systems such as CommCare, used by community health workers to collect and manage health data during home visits.
5. Human Resources for Health Information Systems, designed for managing data on healthcare staff, such as iHRIS.
6. Telemedicine Platforms which enable remote consultations and the sharing of medical information between healthcare providers and patients.

APPENDIX 4: LIST OF THE PATIENT HEALTH DATA PROTECTION PRINCIPLES

From the Uganda Data Protection and Privacy Act, 2019:

1. Accountability - The healthcare worker/hospital is responsible for handling patient health data lawfully.
2. Lawfulness, fairness and consent - Data should only be collected with legal justification, normally with patient consent.
3. Data minimization - Collect only what is necessary for the clinical purpose.
4. Accuracy - Ensure data is correct, complete, uncorrupted and up to date.
5. Retention limitation - Keep data only as long as necessary, then delete/securely dispose of it.
6. Transparency and patient participation - Inform patients about what data is collected, why, and their rights (access, correction).
7. Security safeguards - Protect data against unauthorized access, loss, alteration, or destruction.
8. Confidentiality - Patient health data must not be disclosed unlawfully or inappropriately.

APPENDIX 5: LIST OF PATIENT HEALTH DATA PROTECTION PRACTICES

Expected Healthcare workers' Patient health data Protection Practices. These are the actions healthcare workers should perform to show compliance.

Data Access and Confidentiality Practices

1. Consent and lawful use - Obtain patient consent before recording or sharing their health information.
2. Minimal data collection - Record only relevant patient details needed for treatment or reporting.
3. Patient transparency - Explain to patients why their data is being collected and how it was used.
4. Confidential handling - Avoid discussing or exposing patient information to unauthorized persons.

Authentication and Authorization Practices

5. Use of secure access controls - Use strong passwords, avoid sharing logins and log out of systems after use.

Data Security and System Protection Practices

6. Ensuring accuracy - Cross-check and update patient health data regularly to avoid errors.
7. Secure retention and disposal -Store patient files only for the required time and ensure secure destruction/disposal when no longer needed.
8. Secure communication - Use hospital-approved systems for transmitting patient health data, not personal email/WhatsApp.
9. Physical security -Keep records/devices safe (lockable cabinets, password-protected computers, secured workstations).

Data Integrity and Incident Management Practices

10. Breach reporting - Immediately report suspected data breaches or unauthorized access.

APPENDIX 6: INFORMED CONSENT FORM

Topic of the Study: Healthcare Workers' Knowledge of Patient Health Data Protection When Using Digital Health Solutions at Hoima Regional Referral Hospital

No	Name of Investigator	Designation	Address/ Telephone/ Email	Institution of Affiliation
1	Jacqueline Ainabyoona	Principle investigator	jacqueaina@gmail.com	Uganda Christian University, Mukono (Main Campus)
2	Dr. Edward Kibikyo Mukooza	Co-investigator/Academic Supervisor	emukooza@ucu.ac.ug	Uganda Christian University, Mukono (Main Campus)

Introduction

This study is being conducted by Jacqueline Ainabyoona, a candidate pursuing a master's degree in public health from Uganda Christian University, Uganda. The researcher is interested in identifying the digital health solutions used by healthcare workers, their knowledge of patient health data protection when using the digital health solutions and their patient health data protection practices in the use of digital health solutions at Hoima Regional Referral Hospital (HRRH). You are being asked to participate because you are a healthcare worker at HRRH with valuable insights and experiences that can contribute to this research.

Description of the Research

The purpose of this study is to help the researcher to examine healthcare workers' knowledge of patient health data protection when using digital health solutions at Hoima Regional Referral Hospital by identifying the digital health solutions used by healthcare workers at Hoima Regional Referral Hospital, assessing the healthcare workers' knowledge of patient health data protection when using digital health solutions and describing the patient health data protection practices of healthcare workers when using digital health solutions.

Who Will Participate and why in the Study?

Healthcare workers and these include Doctors, nurses, records officers, laboratory technicians, midwives, dentists and Clinical officers at HRRH are invited to participate in this study. The researcher aims to gather diverse perspectives to gain a comprehensive understanding of the knowledge of patient health data protection among healthcare workers using digital health solutions at Hoima Regional Referral Hospital

Potential Risks and Discomforts

There are no anticipated risks or discomforts associated with participating in this study. However, if any question makes you uncomfortable, you have the right to skip that question or withdraw from the study at any time.

Potential Benefits

While there may not be direct benefits to you, your participation will contribute to the researcher's understanding of the knowledge of patient health data protection among healthcare workers using digital health solutions at Hoima Regional Referral Hospital.

Confidentiality

Your responses was confidential, and your personal information will not be shared with anyone outside the research team. Your responses was stored securely and will only be used for the purposes of this research.

Procedure

If you agree to participate, you was asked to complete a questionnaire and as well be interviewed as guided. The questionnaire will include questions about the digital health solutions you use, your knowledge of patient health data protection when using the digital health solutions and your patient health data protection practices in the use of digital health solutions at Hoima Regional Referral Hospital (HRRH). The questionnaire should take approximately 15 minutes to complete.

Voluntary Participation or Statement of Voluntariness

Your participation is completely voluntary and you will not be compensated for your time. If you decide to participate, you can withdraw at any time. Your decision to participate, decline or withdraw will not affect your relationship with Uganda Christian University.

Withdrawal from the study and withdrawal of Authorization

Participation in this study is voluntary. You have the right to decline to participate or withdraw at any time without penalty. There are no consequences for choosing not to participate or for leaving the study early.

Reimbursements or Cost

There is no cost to participate in this study. Your participation is completely voluntary and you will not be compensated for your time.

Whom to contact in case of ethical related concerns?

This study was approved by Uganda Christian national council for Science and Technology (UNCST), In case of any Ethical or your rights related concerns or inquiries, please contact UCUREC Chairperson; Prof. Peter Waiswa, 0772405357, pwaiswa@musph.ac.ug or UCUREC Manager, Mr. Osborn Ahimbisibwe, 0775737627 or oahimbisibwe@ucu.ac.ug UNCST: Tel; +256414705500, info@uncst.go.ug

STATEMENT OF CONSENT

Do you accept to be recorded?

Yes ☐ No ☐

I voluntary agree to participate in this research program to tick appropriately.

Yes ☐ No ☐

I understand that I was given a copy of this consent form.

Name of Participant:

Sign: Date:

Name of Researcher:

Sign..... Date.....

APPENDIX 7: RESEARCH ETHICS COMMITTEE APPROVAL LETTER



UGANDA CHRISTIAN UNIVERSITY

A Centre of Excellence in the Heart of Africa



10/11/2025

Office of the Vice Chancellor
Research Ethics Committee UG-026

To: Jacqueline Ainabyoona
UgandaChristianUniversity



Review Type: Initial Review

Re:UCUREC-2025-204: HEALTHCARE WORKERS' KNOWLEDGE OF PATIENT HEALTH DATA PROTECTION WHEN USING DIGITAL HEALTH SOLUTIONS AT HOIMA REGIONAL REFERRAL HOSPITAL

I am pleased to inform you that the Uganda Christian University REC, through expedited review held on **06/11/2025** approved the above referenced study.

Approval of the research is for the period of **10/11/2025 to 10/11/2026**.

As Principal Investigator of the research, you are responsible for fulfilling the following requirements of approval:

1. All co-investigators must be kept informed of the status of the research.
2. Changes, amendments, and addenda to the protocol or the consent form must be submitted to the REC for re-review and approval **prior** to the activation of the changes.
3. Reports of unanticipated problems involving risks to participants or any new information which could change the risk benefit: ratio must be submitted to the REC.
4. Only approved consent forms are to be used in the enrollment of participants. All consent forms signed by participants and/or witnesses should be retained on file. The REC may conduct audits of all study records, and consent documentation may be part of such audits.
5. Continuing review application must be submitted to the REC **eight weeks** prior to the expiration date of **10/11/2026** in order to continue the study beyond the approved period. Failure to submit a continuing review application in a timely fashion may result in suspension or termination of the study.
6. The REC application number assigned to the research should be cited in any correspondence with the REC of record.
7. You are required to register the research protocol with the Uganda National Council for Science and Technology (UNCST) for final clearance to undertake the study in Uganda.

The following is the list of all documents approved in this application by Uganda Christian University REC:

No.	Document Title	Language	Version Number	Version Date
1	Protocol	English	one	2025-10-21
2	Data collection tools	English	one	2025-10-21
3	Main Consent forms	English	one	2025-10-21

Research and Ethics

P.O. Box 4, Mukono, Uganda, Plot 67-173, Bishop Tucker Road, Mukono Hill
Tel: +256 (0) 312 350 885 Fax: +256 (0) 4142 90 800 Email: rec@ucu.ac.ug Web: www.ucu.ac.ug
UCUREC is accredited by Uganda National Council for Science & Technology, FDA, and National Institutes for Health of the United States of America

Yours sincerely

Prof. Peter Waiswa
For: Uganda Christian University REC



**UGANDA CHRISTIAN
UNIVERSITY**

A Centre of Excellence in the Heart of Africa

Office of the Vice Chancellor
Research Ethics Committee UG-026



Research and Ethics

P.O. Box 4, Mukono, Uganda, Plot 67-173, Bishop Tucker Road, Mukono Hill
Tel: +256 (0) 312 350 885 Fax: +256 (0) 4142 90 800 Email: rec@ucu.ac.ug Web: www.ucu.ac.ug
UCUREC is accredited by Uganda National Council for Science & Technology, FDA, and National Institutes for Health of the United States of America